C. R. Acad. Sci. Paris, Ser. I 353 (2015) 683–688

Contents lists available at ScienceDirect

C. R. Acad. Sci. Paris, Ser. I

www.sciencedirect.com

Number theory

The truth about torsion in the CM case

La vérité sur la torsion dans le cas CM

Pete L. Clark, Paul Pollack

Department of Mathematics, University of Georgia, Athens, GA, 30602, USA

ARTICLE INFO

Article history:
Received 9 March 2015
Accepted after revision 22 May 2015
Available online 2 July 2015

Presented by Jean-Pierre Serre

ABSTRACT

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

RÉSUMÉ

Soit $T_{CM}(d)$ la taille maximale du sous-groupe de torsion d'une courbe elliptique à multiplications complexes, définie sur un corps de nombres de degré d. Nous montrons qu'il existe C une constante absolue, effective, telle que $T_{CM}(d) \le Cd \log\log(d)$ pour tout $d \ge 3$.

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 $d \ge 3$ and all elliptic curves $E_{/F}$ with complex multiplication,*

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

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

Theorem 2. *(See Hindry–Silverman [9].) For all number fields F of degree $d \ge 2$ and all elliptic curves $E_{/F}$ with j-invariant $j(E) \in \mathcal{O}_F$, we have*

$$\#E(F)[\text{tors}] \le 1\,977\,408 d \log d.$$

E-mail addresses: plclark@gmail.com (P.L. Clark), pollack@uga.edu (P. Pollack).

http://dx.doi.org/10.1016/j.crma.2015.05.004

Every CM elliptic curve $E_{/F}$ has $j(E) \in \mathcal{O}_F$, and only finitely many $j \in \mathcal{O}_F$ are j-invariants of CM elliptic curves $E_{/F}$. But the improvement of $\log\log d$ over $\log d$ is interesting in view of the following result.

Theorem 3. *(See Breuer [4].) Let $E_{/F}$ be an elliptic curve over a number field. There exists a constant $c(E, F) > 0$, integers $3 \le d_1 < d_2 < \ldots < d_n < \ldots$ and number fields $F_n \supset F$ with $[F_n : F] = d_n$ such that for all $n \in \mathbb{Z}^+$ we have*

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

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

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

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 $T_{\mathbf{CM}}(d)$ but replacing “CM elliptic curve” with “elliptic curve”, and define $T_{\neg\mathbf{CM}}(d)$ as for $T_{\mathbf{CM}}(d)$ but replacing “CM elliptic curve” with “elliptic curve *without* CM”. Hindry and Silverman ask whether $T_{\neg\mathbf{CM}}(d)$ has upper order $\sqrt{d \log\log d}$. If so, the upper order of $T(d)$ would be $d \log\log d$ [5, Conjecture 1].

2. Proof of the Main Theorem

2.1. Torsion points and ray class containment

Let K be a number field. Let $\mathcal{O}_K$ be the ring of integers of K, Δ_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 $\mathcal{O}_K$” we shall always mean a nonzero ideal. For an ideal $\mathfrak{a}$ of $\mathcal{O}_K$, we write $K^{(\mathfrak{a})}$ for the $\mathfrak{a}$-ray class field of K. We also put $|\mathfrak{a}| = \#\mathcal{O}_K/\mathfrak{a}$ and

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

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

Lemma 4. *Let K be an imaginary quadratic field and $\mathfrak{a}$ an ideal of $\mathcal{O}_K$. Then*

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

Proof. This follows from [6, Corollary 3.2.4]. $\square$

Theorem 5. *Let K be an imaginary quadratic field, $F \supset K$ 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 $F \supset K^{(N\mathcal{O}_K)}$.*

Proof. The result is part of classical CM theory when $\operatorname{End} E = \mathcal{O}_K$ is the maximal order in K [15, II.5.6]. We shall reduce to that case. There is an $\mathcal{O}_K$-CM elliptic curve $E'_{/F}$ and a canonical F-rational isogeny $\iota\colon E \to E'$ [5, Prop. 25]. There is a field embedding $F \hookrightarrow \mathbb{C}$ such that the base change of ι to $\mathbb{C}$ is, up to isomorphisms on the source and target, given by $\mathbb{C}/\mathcal{O} \to \mathbb{C}/\mathcal{O}_K$. If we put

$$P = 1/N + \mathcal{O} \in E[N], \quad P' = 1/N + \mathcal{O}_K \in E'[N],$$

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

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 $K^{(N\mathcal{O}_K)}$.

2.2. Squaring the torsion subgroup of a CM elliptic curve

Theorem 7. *Let K be an imaginary quadratic field, let $F \supset K$ 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 $[F(E[ab]) : F] \le b$.*

Proof. Step 1: Let $\mathcal{O} = \operatorname{End} E$. For $N \in \mathbb{Z}^+$, let $C_N = (\mathcal{O}/N\mathcal{O})^\times$. Let $E[N] = E[N](\overline{F})$. As an $\mathcal{O}/N\mathcal{O}$-module, $E[N]$ is free of rank 1. Let $\mathfrak{g}_F = \operatorname{Aut}(\overline{F}/F)$, and let $\rho_N : \mathfrak{g}_F \longrightarrow \mathrm{GL}_2(\mathbb{Z}/N\mathbb{Z})$ be the mod N Galois representation associated with $E_{/F}$. Because E has $\mathcal{O}$-CM and $F \supset K$, we have

$$\rho_N : \mathfrak{g}_F \longrightarrow \operatorname{Aut}_{\mathcal{O}} E[N] \cong \mathrm{GL}_1(\mathcal{O}/N\mathcal{O}) \cong (\mathcal{O}/N\mathcal{O})^\times = C_N.$$

Let Δ 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 $\alpha e_1 + \beta e_2 \mapsto \begin{bmatrix} \alpha & \frac{\beta\Delta-\beta\Delta^2}{4} \\ \beta & \alpha+\beta\Delta \end{bmatrix}$. So

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

From this we easily deduce the following useful facts:

(i) C_N contains the homotheties $\left\{ \begin{bmatrix} \alpha & 0 \\ 0 & \alpha \end{bmatrix} \mid \alpha \in (\mathbb{Z}/N\mathbb{Z})^\times \right\}$.
(ii) For all primes p and all $A, B \ge 1$, the natural reduction map $C_{p^{A+B}} \to C_{p^A}$ 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 $A \ge 0$ and $B \ge 1$. 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 $[F(E[p^{A+1}]) : F] \le p$.

Case $A = 0$:

- If $\left(\frac{\Delta}{p}\right) = 1$, then C_p is conjugate to $\left\{ \begin{bmatrix} \alpha & 0 \\ 0 & \beta \end{bmatrix} \mid \alpha, \beta \in \mathbb{F}_p^\times \right\}$. If $\alpha \ne 1$ (resp. $\beta \ne 1$) the only fixed points $(x, y) \in \mathbb{F}_p^2$ of $\begin{bmatrix} \alpha & 0 \\ 0 & \beta \end{bmatrix}$ have $x = 0$ (resp. $y = 0$). Because $E(F)$ contains a point of order p we must either have $\alpha = 1$ for all $\begin{bmatrix} \alpha & 0 \\ 0 & \beta \end{bmatrix} \in \rho_p(\mathfrak{g}_F)$ or $\beta = 1$ for all $\begin{bmatrix} \alpha & 0 \\ 0 & \beta \end{bmatrix} \in \rho_p(\mathfrak{g}_F)$. Either way, $\#\rho_p(\mathfrak{g}_F) \mid p-1$.
- If $\left(\frac{\Delta}{p}\right) = -1$, 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 $\#\rho_p(\mathfrak{g}_F) = 1$.
- If $\left(\frac{\Delta}{p}\right) = 0$, then C_p is conjugate to $\left\{ \begin{bmatrix} \alpha & \beta \\ 0 & \alpha \end{bmatrix} \mid \alpha \in \mathbb{F}_p^\times,\ \beta \in \mathbb{F}_p \right\}$ [3, §4.2]. Since $E(F)$ has a point of order p, every element of $\rho_p(\mathfrak{g}_F)$ has 1 as an eigenvalue and thus $\rho_p(\mathfrak{g}_F) \subset \left\{ \begin{bmatrix} 1 & \beta \\ 0 & 1 \end{bmatrix} \mid \beta \in \mathbb{F}_p \right\}$, so has order dividing p.

Case $A \ge 1$: 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 $\rho_{p^{A+1}}(\mathfrak{g}_F) \subset \mathcal{K}$. Since $E(F)$ has a point of order p^{A+1}, by (i) the homothety $\begin{bmatrix} 1+p^A & 0 \\ 0 & 1+p^A \end{bmatrix}$ lies in $\mathcal{K} \setminus \rho_{p^{A+1}}(\mathfrak{g}_F)$. Therefore $\rho_{p^{A+1}}(\mathfrak{g}_F) \subsetneq \mathcal{K}$, so $\#\rho_{p^{A+1}}(\mathfrak{g}_F) \mid p$. $\square$

2.3. Uniform bound for Euler's function in imaginary quadratic fields

Let $\mathfrak{a}$ be an ideal in an imaginary quadratic field K. To apply the results of Section 2.1, we require a lower bound on $\frac{\varphi_K(\mathfrak{a})}{|\mathfrak{a}|}$. For *fixed* K, it is straightforward to adapt a classical argument of Landau (see the proof of [10, Theorem 328, p. 352]). Replacing Landau's use of Mertens' Theorem with Rosen's number field analogue [13], one obtains the following result: let γ denote the Euler–Mascheroni constant, and let $\chi(\cdot) = (\frac{\Delta_K}{\cdot})$ be the quadratic Dirichlet character associated with K. Then

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

Alas, 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 [2, (4′)]). Second, it only addresses limiting behavior as $|\mathfrak{a}| \to \infty$. However, looking back at Lemma 4 we see that a lower bound on $h_K \frac{\varphi_K(\mathfrak{a})}{|\mathfrak{a}|}$ 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 $\mathfrak{a}$ of $\mathcal{O}_K$ with $|\mathfrak{a}| \ge 3$, we have*

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

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

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

Proof. By the quadratic class number formula, $h_K \asymp L(1,\chi)\sqrt{|\Delta|}$ [7, eq. (15), p. 49]. Writing $L(1,\chi) = \prod_p (1-\chi(p)/p)^{-1}$ and rearranging, we see (1) holds iff

$$\prod_{p > x}\left(1 - \frac{\chi(p)}{p}\right) \ll \sqrt{|\Delta|}, \tag{2}$$

with an effective and absolute implied constant. By Mertens' Theorem [10, 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 $S(t) := \sum_{p \leq t}\chi(p)\log p = -t^\beta/\beta + O(t/\log t)$, where the main term is present only if $L(s,\chi)$ has a Siegel zero β. (Cf. [7, eq. (8), p. 123].) We will assume the Siegel zero exists; otherwise the argument is similar but simpler. By partial summation,

$$\begin{aligned}\sum_{p>y}\frac{\chi(p)}{p} &= -\frac{S(y)}{y\log y} + \int_y^\infty \frac{S(t)}{t^2(\log t)^2}(1+\log t)\,\mathrm{d}t \\ &\ll 1 + \int_y^\infty \frac{t^\beta}{t^2\log t}\,\mathrm{d}t.\end{aligned}$$

Haneke, Goldfeld–Schinzel, and Pintz have each shown that $\beta \leq 1 - c/\sqrt{|\Delta|}$, where the constant $c > 0$ is absolute and effective [8,11,12]. Using this to bound t^β, and keeping in mind that $y \geq \exp(\sqrt{|\Delta|})$, we see that the final integral is at most

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

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

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

$$\frac{\varphi_K(\mathfrak{a})}{|\mathfrak{a}|} \geq \prod_{|\mathfrak{p}|\leq z}\left(1 - \frac{1}{|\mathfrak{p}|}\right). \tag{3}$$

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 9 yield

$$\begin{aligned}\prod_{|\mathfrak{p}|\leq z}\left(1-\frac{1}{|\mathfrak{p}|}\right) &\geq \prod_{p\leq z}\left(1-\frac{1}{p}\right)\left(1-\frac{(\frac{\Delta}{p})}{p}\right) \\ &\gg (\log z)^{-1}\prod_{p\leq z}\left(1-\frac{(\frac{\Delta}{p})}{p}\right) \gg (\log z)^{-1}\cdot h_K^{-1}.\end{aligned} \tag{4}$$

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

$$z = (C'\log|\mathfrak{a}|)^2. \tag{5}$$

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

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

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

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

2.4. Proof of Theorem 1

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

$$2d \ge [FK:\mathbb{Q}] \ge [K^{(a\mathcal{O}_K)}:\mathbb{Q}] \ge \frac{h_K\varphi_K(a\mathcal{O}_K)}{3}.$$

By Theorem 7, there is an extension L/FK with $(\mathbb{Z}/ab\mathbb{Z})^2 \hookrightarrow E(L)$ and $[L:FK] \le b$. Applying Theorem 5 and Lemma 4 as above we get $L \supset K^{(ab\mathcal{O}_K)}$ and

$$[L:\mathbb{Q}] \ge [K^{(ab\mathcal{O}_K)}:\mathbb{Q}] \ge \frac{h_K\varphi_K(ab\mathcal{O}_K)}{3},$$

so

$$d = [F:\mathbb{Q}] \ge \frac{[FK:\mathbb{Q}]}{2} = \frac{[L:\mathbb{Q}]}{2[L:FK]} \ge \frac{[L:\mathbb{Q}]}{2b} \ge \frac{h_K\varphi_K(ab\mathcal{O}_K)}{6b}. \tag{6}$$

Multiplying (6) through by $(ab)^2 = |ab\mathcal{O}_K|$ and rearranging, we get

$$\#E(FK)[\mathrm{tors}] = a^2b \le 6\frac{d}{h_K}\frac{|ab\mathcal{O}_K|}{\varphi_K(ab\mathcal{O}_K)}. \tag{7}$$

By Theorem 8 we have

$$\frac{|ab\mathcal{O}_K|}{\varphi_K(ab\mathcal{O}_K)} \ll h_K \log\log|ab\mathcal{O}_K| \le h_K \log\log(a^2b)^2 \ll h_K \log\log \#E(FK)[\mathrm{tors}]. \tag{8}$$

Combining (7) and (8) gives

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

and thus

$$\#E(F)[\mathrm{tors}] \le \#E(FK)[\mathrm{tors}] \ll d\log\log d.$$

3. Related work

Let E be a K-CM elliptic curve defined over a number field F, and let $P \in E(F)[\mathrm{tors}]$. Silverberg showed [14, Corollary 6.1] that if $F \supset K$ then $\varphi(\#\langle P\rangle) \le 3[F:\mathbb{Q}]$. It follows that if $F \not\supset K$ then $\varphi(\#\langle P\rangle) \le 6[F:\mathbb{Q}]$. Later Aoki showed [1, Proposition 8.1] that if $F \not\supset K$ then $\varphi(\#\langle P\rangle) \le 2[F:\mathbb{Q}]$. Silverberg's and Aoki's bounds are *the real truth*: there are points of order 6 when $F = \mathbb{Q}$ and of order 7 when $F = K = \mathbb{Q}(\sqrt{-3})$.

These results give an $O(d\log\log d)$ bound on the *exponent* of $E(F)[\mathrm{tors}]$ and thus imply $\#E(F)[\mathrm{tors}] = O((d\log\log d)^2)$, which was later superseded by Theorem 2. If $F \not\supset K$, then $E(F)[\mathrm{tors}]$ has a cyclic subgroup of index at most 2. Thus the work of Silverberg and Aoki yields Theorem 1 when $F \not\supset K$, in fact in the more explicit form

$$\#E(F)[\mathrm{tors}] \le (4\,\mathrm{e}^{\gamma} + o(1))d\log\log d, \qquad \text{as } d \to \infty.$$

Acknowledgments

We thank John Voight for suggesting that the proof of Theorem 1 ought to be in reach, Alice Silverberg for providing pointers to the literature, and the referee for a rapid, careful reading accompanied by useful comments. We are extremely grateful to Abbey Bourdon for pointing out an error in a previous draft. The second author is supported by NSF award DMS-1402268.

References

[1] N. Aoki, Torsion points on abelian varieties with complex multiplication, in: Algebraic Cycles and Related Topics, Kitasakado, 1994, World Sci. Publ., River Edge, NJ, USA, 1995, pp. 1–22.

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

[3] A. Bourdon, P.L. Clark, J. Stankewicz, Torsion points on CM elliptic curves over real number fields, submitted for publication, http://arxiv.org/abs/1411.2742.

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

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

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

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

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

[9] M. Hindry, J. Silverman, Sur le nombre de points de torsion rationnels sur une courbe elliptique, C. R. Acad. Sci. Paris, Ser. I 329 (2) (1999) 97–100.

[10] G.H. Hardy, E.M. Wright, An Introduction to the Theory of Numbers, sixth edition, Oxford University Press, Oxford, UK, 2008.

[11] D.M. Goldfeld, A. Schinzel, On Siegel's zero, Ann. Sc. Norm. Super. Pisa, Cl. Sci. (4) 2 (1975) 571–583.

[12] 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.

[13] M. Rosen, A generalization of Mertens' theorem, J. Ramanujan Math. Soc. 14 (1999) 1–19.

[14] A. Silverberg, Points of finite order on abelian varieties, in: p-Adic Methods in Number Theory and Algebraic Geometry, in: Contemp. Math., vol. 133, Amer. Math. Soc., Providence, RI, USA, 1992, pp. 175–193.

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