ACYCLOTOMY OF TORSION IN THE CM CASE

PETE L. CLARK

ABSTRACT. We show that as F ranges over all abelian number fields and $E_{/F}$ ranges over all elliptic curves with complex multiplication, the size of the torsion subgroup $E(F)[\mathrm{tors}]$ is uniformly bounded.

NOTATION

For a field F, we write F^{sep} for a separable algebraic closure and $\mathfrak{g}_F$ for $\mathrm{Aut}(F^{\mathrm{sep}}/F)$. We identify finite étale group schemes $G_{/F}$ with their associated $\mathfrak{g}_F$-modules $G(F^{\mathrm{sep}})$. For a number field F, let $F^{\mathrm{cyc}} = \bigcup_{n \geq 1} F(\zeta_n)$, and let F^{ab} be the maximal abelian extension of F. When $F = \mathbb{Q}$, $F^{\mathrm{cyc}} = F^{\mathrm{ab}}$: the Kronecker-Weber Theorem.

1. INTRODUCTION

In October 2014 I visited Dartmouth College and spoke about results obtained with Bourdon and Stankewicz bounding torsion points of CM elliptic curves defined over real number fields [BCS14]. On the morning of my departure John Voight urged further consideration of the cyclotomic case. The return trip was lengthy, and by the time I arrived in Atlanta I had obtained the following result.

Main Theorem. *There is $T \in \mathbb{Z}^+$ such that for every CM elliptic curve $E_{/\mathbb{Q}^{\mathrm{ab}}}$,*

$$\#E(\mathbb{Q}^{\mathrm{ab}})[\mathrm{tors}] \leq T.$$

The following day I made some extensions by incorporating results of Zarhin, and I communicated these results to Bourdon and Voight in the form of a "letter."

I had hoped to carry these results further and in particular to go from a boundedness theorem to a complete classification. However, in the intervening time our work on torsion in the CM case has become focused in other directions: truth [CP15], anatomy [BCP15] and oddity [BP15]. So I have decided to publish this modest venture into "acyclotomy" essentially as written in my 11/1/2014 letter.

We say $j \in \mathbb{C}$ is a **singular modulus** if there is an elliptic curve $E_{/\mathbb{C}}$ with $j(E) = j$ and complex multiplication; otherwise we say j is a **nonsingular modulus**. We say $j \in \mathbb{C}$ is an **abelian modulus** if $\mathbb{Q}(j)/\mathbb{Q}$ is an abelian algebraic extension.

Lemma 1. *There are only finitely many abelian singular moduli. Conditionally on the Generalized Riemann Hypothesis (GRH), they comprise* 101 *Galois orbits.*

Proof. The map which associated to any imaginary quadratic order $\mathcal{O}$ the Galois orbit of $j(\mathbb{C}/\mathcal{O})$ gives a bijection from the set of imaginary quadratic orders to the set of Galois orbits of singular moduli. Whether a singular modulus is abelian depends only on its Galois orbit. Let K be the fraction field of the imaginary

Date: March 5, 2016.

quadratic order $\mathcal{O}$. The modulus $j_{\mathcal{O}} = j(\mathbb{C}/\mathcal{O})$ is abelian iff $K(j_{\mathcal{O}})/\mathbb{Q}$ is abelian. Moreover we have [C, Lemma 9.3] that $K(j_{\mathcal{O}})/\mathbb{Q}$ is Galois,

$$\mathrm{Aut}(K(j(\mathbb{C}/\mathcal{O}))/K) \cong \mathrm{Pic}\,\mathcal{O},$$

and

$$\mathrm{Aut}(K(j(\mathbb{C}/\mathcal{O}))/\mathbb{Q}) \cong \mathrm{Aut}(K(j(\mathbb{C}/\mathcal{O}))/K) \rtimes (\mathbb{Z}/2\mathbb{Z}) \cong \mathrm{Pic}\,\mathcal{O} \rtimes (\mathbb{Z}/2\mathbb{Z}); \quad (1)$$

the action of $\mathbb{Z}/2\mathbb{Z}$ on $\mathrm{Pic}\,\mathcal{O}$ is by inversion. So $j_{\mathcal{O}}$ is an abelian modulus iff $\mathrm{Pic}\,\mathcal{O} = (\mathrm{Pic}\,\mathcal{O})[2]$. Heilbronn showed $\frac{\#\,\mathrm{Pic}\,\mathcal{O}}{\#(\mathrm{Pic}\,\mathcal{O})[2]}$ approaches infinity as $\mathcal{O}$ ranges over all imaginary quadratic orders [He34], so there are only finitely many abelian singular moduli. Conditionally on GRH, J. Voight has computed the complete list of $\mathcal{O}$ such that $\mathrm{Pic}\,\mathcal{O}$ has exponent dividing 2 [Vo07]:[1] there are 101 such orders. □

So to prove the Main Theorem it suffices to show that for each imaginary quadratic order $\mathcal{O}$ such that $j(\mathbb{C}/\mathcal{O})$ is an abelian modulus, there is an absolute bound on $\#E(\mathbb{Q}^{\mathrm{ab}})[\mathrm{tors}]$ for $\mathcal{O}$-CM elliptic curves $E_{/\mathbb{Q}^{\mathrm{ab}}}$. This leads to a problem that makes sense for all elliptic curves, and in the non-CM case we can prove a stronger result.

Theorem 2. *Let $j \in \overline{\mathbb{Q}}$ be a nonsingular modulus, and let F be a number field containing j. Then there is a positive integer $T = T(F, j)$ such that for every elliptic curve $E_{/F^{\mathrm{ab}}}$ with $j(E) = j$, we have $\#E(F^{\mathrm{ab}})[\mathrm{tors}] \leq T$.*

The conclusion of Theorem 2 is false for all singular moduli: if K is the CM field, take $F = K(j)$. Then for any elliptic curve $E_{/F}$, $E(F^{\mathrm{ab}})[\mathrm{tors}] = E(\mathbb{C})[\mathrm{tors}] \cong (\mathbb{Q}/\mathbb{Z})^2$. In the CM case the result can be salvaged by replacing F^{ab} with F^{cyc}.

Theorem 3. *Let $j \in \overline{\mathbb{Q}}$ be a singular modulus with corresponding CM field K. Let $F \supset K(j)$ be a number field. Then there is a positive integer $T = T(F, j)$ such that for every elliptic curve $E_{/F^{\mathrm{cyc}}}$ with $j(E) = j$, we have $\#E(F^{\mathrm{cyc}})[\mathrm{tors}] \leq T$.*

Since for a K-CM elliptic curve E, $j(E)$ is an abelian modulus iff $K(j(E))^{\mathrm{cyc}} = \mathbb{Q}^{\mathrm{ab}}$, Lemma 1 and Theorem 3 imply the Main Theorem.

We will prove Theorems 2 and 3 in §2. In §3 we end with some open questions.

Acknowledgments: Thanks to John Voight for asking the question that inspired this note and to Abbey Bourdon and James H. Stankewicz for helpful comments.

2. The Proofs

2.1. **The Basic Strategy.**

Let $\{(A_i)_{/F_i}\}_{i \in I}$ be a family of abelian varieties defined over fields F_i, of uniformly bounded dimension. Then $\sup_{i \in I} \#A_i(F_i)[\mathrm{tors}] < \infty$ iff both of the following hold:

(B1) The set of primes ℓ dividing some $\#A_i(F_i)[\mathrm{tors}]$ is finite; and
(B2) For all primes ℓ, there is $a \in \mathbb{Z}^+$ such that no $A_i(F_i)$ has a point of order ℓ^a.

[1]The published version contains a minor error in the tables. A corrected version is available at `http://arxiv.org/abs/math/0410266`.

We will prove Theorems 2 and 3 by verifying conditions (B1) and (B2). Moreover we will make use of the following seminal results on torsion points on abelian varieties over abelian extensions of number fields.

Theorem 4. *Let $A_{/F}$ be an abelian variety over a number field.*
a) (Ribet [KL81]*) Then $A(F^{\mathrm{cyc}})[\mathrm{tors}]$ is finite.*
b) (Zarhin [Za87]*) Write $A = \prod_{i=1}^n A_i$ with each A_i an F-simple variety. The following are equivalent:*
(i) The group $A(F^{\mathrm{ab}})$ is finite.
(ii) For all $1 \leq i \leq n$, $\mathrm{End}_F A_i$ is not an order in a number field of degree $2 \dim A_i$.

2.2. **Condition (B1).** Suppose j is a nonsingular modulus. Let F be a number field containing j, and let $E_{/F}$ be an elliptic curve with $j(E) = j$. By Serre's Open Image Theorem [S72, Thm. 3], there is $L = L(E, F)$ such that for all primes $\ell \geq \max(L, 5)$, the mod ℓ Galois representation

$$\rho_\ell : \mathfrak{g}_F \to \mathrm{GL}_2(\mathbb{Z}/\ell\mathbb{Z})$$

is surjective. We will show that for all such ℓ, for any elliptic curve $E'_{/F^{\mathrm{ab}}}$ with $j(E') = j$, $E'(F^{\mathrm{ab}})[\ell] = 0$. Indeed, suppose not: then $E' = E^t$ is a quadratic twist of E by some $t \in (F^{\mathrm{ab}})^\times$, so E has a point of order ℓ rational over $F^{\mathrm{ab}}(\sqrt{t})$. Consider the following tower of fields:

$$F \subset F^{\mathrm{ab}} \subset F^{\mathrm{ab}}(\sqrt{t}) \subset F^{\mathrm{ab}}(\sqrt{t}, E[\ell]).$$

At each step in the tower we have a solvable extension; this is immediate for all steps except the last. For that: since we have a point of order ℓ defined over $F^{\mathrm{ab}}(\sqrt{t})$, the image of the mod ℓ Galois representation on E when restricted to this field lies in $\{\begin{pmatrix} 1 & b \\ 0 & d \end{pmatrix} \mid b \in \mathbb{Z}/\ell\mathbb{Z}, d \in (\mathbb{Z}/\ell\mathbb{Z})^\times\}$, which is a solvable group. Thus $F^{\mathrm{ab}}(\sqrt{t}, E[\ell])/F$ is solvable, hence its subextension $F(E[\ell])/F$ is solvable. But the latter extension is Galois with group $\mathrm{GL}_2(\mathbb{Z}/\ell\mathbb{Z})$ with $\ell \geq 5$, which has the non-abelian simple group $\mathrm{PSL}_2(\mathbb{Z}/\ell\mathbb{Z})$ as a Jordan-Hölder factor: contradiction.

Suppose j is a singular modulus, with corresponding CM order $\mathcal{O}$ and fraction field K, $F \supset K$ a number field and $E_{/F}$ an $\mathcal{O}$-CM elliptic curve with $j(E) = E$. Suppose $E(F^{\mathrm{cyc}})$ has a point P of order ℓ. For large ℓ we will get a contradiction. Let us suppose first of all that $\ell > |\Delta|$, so ℓ is odd and $\left(\frac{\Delta}{\ell}\right) \neq 0$.
Step 1: We claim E has full ℓ-torsion over F^{cyc}.
• Suppose $\left(\frac{\Delta}{\ell}\right) = -1$. In this case the $\mathcal{O}$-submodule generated by P is all of $E[\ell]$ [CCRS13, Lemma 19]. Since $K \subset F$, this suffices.
• Suppose $\left(\frac{\Delta}{\ell}\right) = 1$. Then there is a $\mathbb{Z}/\ell\mathbb{Z}$-basis P_1, P_2 of $E[\ell]$ such that $\langle P_1 \rangle$ and $\langle P_2 \rangle$ are the only one-dimensional $\mathcal{O}$-stable subspaces of $E[\ell]$, so if $P \notin \langle P_1 \rangle \cup \langle P_2 \rangle$ then the $\mathcal{O}$-submodule generated by P is again $E[\ell]$. So without loss of generality we may assume $P = P_1$, and then the mod ℓ Galois representation over F^{cyc} lies in the subgroup $\{\begin{pmatrix} 1 & 0 \\ 0 & d \end{pmatrix} \mid d \in (\mathbb{Z}/\ell\mathbb{Z})^\times\}$. Since $\det \rho_\ell$ is the mod ℓ cyclotomic character and F^{cyc} contains the ℓth roots of unity, we find that $d = 1$.
Step 2: By [BCS14, Thm. 3.16] for any CM elliptic curve defined over a field F of characteristic zero and containing the CM field K, the torsion field $F(E[\ell])$ contains the ℓ-ray class field $K^{(\ell)}$. Combining this with Step 1, we get

$$F^{\mathrm{cyc}} \supset K^{(\ell)}. \tag{2}$$

Step 3: We will show $[K^{(\ell)}F^{\mathrm{cyc}} : F^{\mathrm{cyc}}]$ tends to infinity with ℓ, contradicting (2) for sufficiently large ℓ and completing the proof. Let $\mathcal{O}_K$ be the ring of integers of K, let Δ_K be its discriminant, and let $\mathcal{O}_\ell$ be the quadratic order of discriminant $\ell^2\Delta_K$. The field $K^{(\ell)}$ contains the ring class field $K(\ell) = K(j(\mathbb{C}/\mathcal{O}_\ell))$. By (1), the maximal abelian subextension of $K(\ell)/\mathbb{Q}$ has degree equal to the order of the abelianization of $\operatorname{Pic}\mathcal{O}_\ell \rtimes \mathbb{Z}/2\mathbb{Z}$, i.e., to $2\#(\operatorname{Pic}\mathcal{O}_\ell[2])$. By [C, Prop. 3.11] we have

$$\#(\operatorname{Pic}\mathcal{O}_\ell[2]) \leq 2\#(\operatorname{Pic}\mathcal{O}_K[2]).$$

Moreover, by [C, Cor. 7.28] we have

$$\frac{\ell - \left(\frac{\Delta}{\ell}\right)}{6} \mid \#\operatorname{Pic}\mathcal{O}_\ell = [K(\ell) : K] = \frac{[K(\ell) : \mathbb{Q}]}{2}.$$

Putting these estimates together, we get

$$[K^{(\ell)}F^{\mathrm{cyc}} : F^{\mathrm{cyc}}] \geq \frac{[K^{(\ell)}\mathbb{Q}^{\mathrm{cyc}} : \mathbb{Q}^{\mathrm{cyc}}]}{[F : \mathbb{Q}]} \geq \frac{[K(\ell)\mathbb{Q}^{\mathrm{cyc}} : \mathbb{Q}^{\mathrm{cyc}}]}{[F : \mathbb{Q}]} \geq \frac{\ell - 1}{12[F : \mathbb{Q}]\#(\operatorname{Pic}\mathcal{O}_K[2])}.$$

2.3. **Condition (B2).**

Lemma 5. *Let F be a field. Let $N > 2$ be indivisible by the characteristic of F.*
a) Let $E_{/F}$ be an elliptic curve and suppose that $E(F)$ has a point of order N. Then at most one nontrivial quadratic twist $E^t_{/F}$ of E has a point of order N.
b) Let $A_{/F}$ be an abelian variety, and suppose that $E(F)$ has a point of order N. Then at most finitely many quadratic twists $A^t_{/F}$ have points of order N.

Proof. a) Without loss of generality we may assume that either $N = \ell > 2$ is a prime or $N = 4$. Either way, let P_1 be a point of order N in $E(F)$. Let $t \in F^\times \setminus F^{\times 2}$ be such that there is $P_2 \in E^t(F)$ of order N. Let $\epsilon_t : \mathfrak{g}_F \to \{\pm 1\}$ be the quadratic character on the absolute Galois group of F corresponding to the quadratic extension $F(\sqrt{t})/F$: because $N > 2$, ϵ_t is nontrivial. The mod N Galois representations on E and E^t are related as follows:

$$\rho_{N,E} = \rho_{N,E^t} \otimes \epsilon_t.$$

Thus, since P_2 is fixed under the action of ρ_{N,E^t}, the image of ρ_N stabilizes the subgoup $\langle P' \rangle$ and under the identification of this group with $\mathbb{Z}/N\mathbb{Z}$ afforded by the basis element P_2, acts on it by the nontrivial quadratic *isogeny character* ϵ_t.

• Suppose $N = \ell$ is an odd prime. Then $\langle P_1, P_2 \rangle = E[\ell](\overline{F})$ and it follows that upon restriction to $F(\sqrt{t})$ the mod N Galois representation is trivial. This rules out a second nontrivial quadratic twist t' which has a point of order N, because that would lead to another nontrivial quadratic isogeny character $\epsilon_{t'}$ which then would not trivialize upon restriction to the Galois group of $F(\sqrt{t})$.

• Suppose $N = 4$. Let $T = E[4](\overline{F})$ and by choosing a basis P_1, Q, identify T with $(\mathbb{Z}/4\mathbb{Z})^2$. If $\langle P_1, P_2 \rangle = T$, we argue as above. However, it may be that $\langle P_1, P_2 \rangle \subsetneq T$: this happens when $\langle P_1 \rangle$ and $\langle P_2 \rangle$ lie in the same fiber of the map $\mathbb{P}^1(\mathbb{Z}/4\mathbb{Z}) \to \mathbb{P}^1(\mathbb{Z}/2\mathbb{Z})$. But all fibers of this map have 2 elements, so if there is a second nontrivial quadratic twist t', this yields a third point $P_3 \in T$ of order 4. Then $\langle P_1, P_3 \rangle = T$. Switching the roles of P_2 and P_3 we argue as above.
b) Replacing "one nontrivial twist" with "finitely many twists," the above argument easily adapts to the case of abelian varieties. □

We immediately deduce the following result.

Proposition 6. *Let F be a field, and let $A_{/F}$ be an abelian variety. Let ℓ be a prime number which is indivisible by the characteristic of F. Suppose $A^t(F)[\ell^\infty]$ is finite for all quadratic twists $A^t_{/F}$ of A, including the "trivial twist" $A^t = A$. Then*

$$\sup_{t \in F^\times/F^{\times 2}} \#A^t(F)[\ell^\infty] < \infty.$$

Let $E_{/F}$ be an elliptic curve over a number field. Suppose $j(E) \neq 0, 1728$, so that every twist of E is a quadratic twist. Then combining Proposition 6 with Theorem 4a) we get that for each prime ℓ, there is $a \in \mathbb{Z}^+$ such that for any elliptic curve $E'_{/F^{\mathrm{cyc}}}$ with $j(E') = j(E)$, we have $E'(F^{\mathrm{cyc}})[\ell^\infty] = E'(F^{\mathrm{cyc}})[\ell^a]$ is a finite group. Similarly, if $j(E)$ is a nonsingular modulus then using Theorem 4b) instead we get that for each prime ℓ, there is $a \in \mathbb{Z}^+$ such that for any elliptic curve $E'_{/F^{\mathrm{ab}}}$ with $j(E') = j(E)$, we have $E'(F^{\mathrm{ab}})[\ell^\infty] = E'(F^{\mathrm{ab}})[\ell^a]$ is a finite group. The same holds when $j(E)$ is a singular modulus and F does not contain the CM field.

It remains to deal with $j = 0, 1728$. For this we use the following result.

Proposition 7. *Let F be a field, and let $N \geq 4$. For any $j \in F$, there are only finitely many F-isomorphism classes of elliptic curves $E_{/F}$ with $j(E) = j$ such that $E(F)$ has a point of order N.*

Proof. This follows from the fact that $Y_1(N)_{/F}$ is a fine moduli scheme for $N \geq 4$. Namely, j induces a closed point on $Y(1)$. The fiber of $Y_1(N) \to Y(1)$ over j contains only finitely many points, which correspond to all F-rational isomorphism classes of pairs (E_i, P_i). with $P_i \in E_i(F)$ of order N. Any elliptic curve over F with $j(E) = j$ and an F-point of order N must be one of these finitely many E_i's. □

Proposition 7 applies to show Condition (B2) in *all* cases, rendering the approach via Lemma 5 logically superfluous. However, when it applies Lemma 5 seems preferable: it gives more precise results and adapts readily to the case of abelian varieties. It would be desirable to supplement it with an analysis of quartic twists (when $j = 1728$) and sextic twists (when $j = 0$)...though we do not so do here.

3. Some Open Questions

3.1. **The non-CM Case.** The motivation of much of the recent work on torsion points in the CM case is that because studying torsion points on CM elliptic curves is so much easier than torsion points on non-CM elliptic curves, it can give a preview as to what to expect in the general case....provided of course that one has reason to believe that the two cases should behave similarly. So it is only natural to ask:

Question 8. *Is there $T \in \mathbb{Z}^+$ such that for all elliptic curves $E_{/\mathbb{Q}^{ab}}$ we have $\#E(\mathbb{Q}^{\mathrm{ab}})[\mathrm{tors}] \leq T$?*

I expect that the answer is "yes." However, whereas our proof of the Main Theorem turns on the finiteness of abelian singular moduli, clearly there are infinitely many abelian nonsingular moduli! So a proof could not proceed in the same way. In fact I do not see how to get started here using extant knowledge and techniques.

3.2. **Abelian varieties.** Theorem 2 is stated for elliptic curves, yet the major technology in its proof – Theorem 4 – holds for abelian varieties. So we ask:

Question 9. *Let F be a number field, and let $A_{/F}$ be an abelian variety. Let $\mathcal{T}(A)$ be the class of all abelian varieties $A'_{/F}$ such that $A'_{/\overline{\mathbb{Q}}} \cong A_{/\overline{\mathbb{Q}}}$.*
a) Do we have $\sup_{A' \in \mathcal{T}(A)} \#A'(F^{\mathrm{cyc}})[\mathrm{tors}] < \infty$?
b) Suppose $A_{/F}$ satisfies condition (ii) of Theorem 4b). Do we have $\sup_{A' \in \mathcal{T}(A)} \#A'(F^{\mathrm{ab}})[\mathrm{tors}] < \infty$?

For abelian varieties of dimension $g \geq 2$, it is no longer true that a rational point of order ℓ forces the mod ℓ Galois representation to have solvable image. However I believe a less crude group-theoretic analysis would yield an answer under the condition that for all sufficiently large primes ℓ, the image of the mod ℓ Galois representation is $\mathrm{GSp}_{2g}(\mathbb{Z}/\ell\mathbb{Z})$. This is the most stringent reasonable interpretation of "no complex multiplication" in the present context, just as Condition (ii) of Theorem 4b) is the most lax. There are many intermediate cases.

3.3. **A full classification.** It would be interesting to sharpen the Main Theorem by classifying torsion subgroups of CM elliptic curves over $\mathbb{Q}^{\mathrm{ab}}$. Our proof reduces this to a finite calculation. However, the actual implementation would be quite challenging: every prime divisor of a class number one CM field occurs as the order of a torsion point of a CM elliptic curve over an abelian number field, so e.g. 163 occurs. So we need to compute an $a \geq 2$ such that no point on $Y_1(163^a)$ in the fiber over $j = -262537412640768000$ has an abelian field of definition. But already the map $Y_1(163^2) \to Y(1)$ has degree 352942596. Perhaps a refined/alternative proof would allow for a less daunting calculation.

References

[BCP15] A. Bourdon, P.L. Clark and P. Pollack, *Anatomy of torsion in the CM case*. To appear, Math. Z. `http://arxiv.org/abs/1506.00565`

[BCS14] A. Bourdon, P.L. Clark and J. Stankewicz, *Torsion points on CM elliptic curves over real number fields*. To appear, Transactions of the AMS. `http://arxiv.org/abs/1411.2742`

[BP15] A. Bourdon and P. Pollack, *Torsion subgroups of CM elliptic curves over odd degree number fields*. `http://arxiv.org/abs/1601.00351`

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

[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.

[CP15] P.L. Clark and P. Pollack, *The truth about torsion in the CM case*. C. R. Math. Acad. Sci. Paris 353 (2015), 683-688.

[He34] H. Heilbronn, *On the Class Number in Imaginary Quadratic Fields*. Quart. J. Math. Oxford Ser. 25 (1934), 150–160.

[KL81] N.M. Katz and S. Lang, *Finiteness theorems in geometric classfield theory*. With an appendix by Kenneth A. Ribet. Enseign. Math. (2) 27 (1981), no. 3–4, 285-319 (1982).

[S72] J.-P. Serre, *Propriétés galoisiennes des points d'ordre fini des courbes elliptiques*. Invent. Math. 15 (1972), no. 4, 259–331.

[Vo07] J. Voight, *Quadratic forms that represent almost the same primes*. Math. Comp. 76 (2007), 1589–1617.

[Za87] Yu. G. Zarhin, *Endomorphisms and torsion of abelian varieties*. Duke Math. J. 54 (1987), 131-145.