A BOUND FOR THE TORSION CONDUCTOR
OF A NON-CM ELLIPTIC CURVE

NATHAN JONES

(Communicated by Ken Ono)

Abstract. Given a non-CM elliptic curve $E$ over $\mathbb{Q}$ of discriminant $\Delta_E$, define the “torsion conductor” $m_E$ to be the smallest positive integer so that the Galois representation on the torsion of $E$ has image $\pi^{-1}(\text{Gal}(\mathbb{Q}(E[m])/\mathbb{Q}))$, where $\pi$ denotes the natural projection $GL_2(\hat{\mathbb{Z}}) \to GL_2(\mathbb{Z}/m_E\mathbb{Z})$. We show that, uniformly for semi-stable non-CM elliptic curves $E$ over $\mathbb{Q}$, one has $m_E \ll \left(\prod_{p|\Delta_E} p\right)^5$.

1. Introduction

Let $E$ be an elliptic curve defined over a number field $K$ and let

$$\varphi_E : \text{Gal}(\overline{K}/K) \to GL_2(\hat{\mathbb{Z}})$$

be the continuous group homomorphism defined by letting $\text{Gal}(\overline{K}/K)$ operate on the torsion points of $E$ and by choosing an isomorphism $\text{Aut}(E_{\text{tors}}) \simeq GL_2(\hat{\mathbb{Z}})$. We will refer to $\varphi_E$ as the torsion representation of $E$. A celebrated theorem of Serre [10] shows that if $E$ has no complex multiplication, then the index of the image of $\varphi_E$ is finite:

$$[GL_2(\hat{\mathbb{Z}}) : \varphi_E(\text{Gal}(\overline{K}/K))] < \infty.$$  

This is equivalent to the statement that there exists an integer $m \geq 1$ with the property that

$$\varphi_E(\text{Gal}(\overline{K}/K)) = \pi^{-1}(\text{Gal}(K(E[m])/K)),$$

where $K(E[m])$ denotes the $m$-th division field of $E$, obtained by adjoining to $K$ the $x$ and $y$ coordinates of the $m$-torsion points of a Weierstrass model of $E$, and where

$$\pi : GL_2(\hat{\mathbb{Z}}) \to GL_2(\mathbb{Z}/m\mathbb{Z})$$

denotes the projection.

Definition 1. We define the torsion conductor $m_E$ of a non-CM elliptic curve $E$ over $K$ to be the smallest positive integer $m$ so that (1) holds.

Serre [10, p. 299] has asked the following important question about the image of $\varphi_E$.

Received by the editors September 6, 2007, and, in revised form, November 25, 2007.
2000 Mathematics Subject Classification. Primary 11G05, 11F80.

©2008 American Mathematical Society
Reverts to public domain 28 years from publication
Question 2. Given a number field $K$, is there a constant $C_K$ such that for any non-CM elliptic curve $E$ over $K$ and any rational prime number $p \geq C_K$ one has

$$\text{Gal}(K(E[p])/K) \simeq GL_2(\mathbb{Z}/p\mathbb{Z}).$$

Even in the case of $K = \mathbb{Q}$ this question remains unanswered. Mazur [7, Theorem 4, p. 131] has shown that

(2) $E$ is semi-stable $\implies \forall p \geq 11$, $\text{Gal}(\mathbb{Q}(E[p])/\mathbb{Q}) \simeq GL_2(\mathbb{Z}/p\mathbb{Z}).$

His work also shows that, if $p > 19$, $p/\in \{37, 43, 67, 163\}$, and

(3) $\text{Gal}(\mathbb{Q}(E[p])/\mathbb{Q}) \subsetneq GL_2(\mathbb{Z}/p\mathbb{Z}),$

then $\text{Gal}(\mathbb{Q}(E[p])/\mathbb{Q})$ is contained in the normalizer of a Cartan subgroup of $GL_2(\mathbb{Z}/p\mathbb{Z})$. The work of Parent [8] represents further progress towards resolution of the split Cartan case, while the work of Chen [2] shows that in the non-split case, new ideas are needed. Other authors have bounded the largest prime $p$ satisfying (3) in terms of invariants of the elliptic curve ([11], [4], [3], and [6]).

In some applications it is useful to have effective control over the variation of $m_E$ with $E$. In this paper we prove the following theorem, whose statement uses the Vinogradov symbol $\ll$, which is defined by

$$A \ll B \iff \exists \text{ an absolute constant } c \text{ such that } |A| \leq cB.$$

Theorem 3. Let $\Delta_E$ denote the minimal discriminant of an elliptic curve $E$ over $\mathbb{Q}$. Then, uniformly for semi-stable non-CM elliptic curves $E$ over $\mathbb{Q}$, one has

$$m_E \ll \left( \prod_{p \text{ prime, } p | \Delta_E} p \right)^5.$$

If Question 2 has an affirmative answer when $K = \mathbb{Q}$, then the above bound holds uniformly for all elliptic curves $E$ over $\mathbb{Q}$.

The proof of Theorem 3 uses elementary Galois theory to reduce the question to working “vertically over exceptional primes” or, in other words, to the analogous question of the Galois representation on the Tate module

$$\text{Gal}(\mathbb{Q}/\mathbb{Q}) \rightarrow GL_2(\mathbb{Z}/p\mathbb{Z}),$$

where $p$ satisfies (3). Such a study has been carried out in the recent work of Arai [1]. The main ideas are present in [9] and [5].

Remark 4. The torsion conductor $m_E$ should not be confused with the number

$$A(E) := 2 \cdot 3 \cdot 5 \cdot \prod_{p \text{ prime, } p \leq \text{Gal}(\mathbb{Q}(E[p])/#GL_2(\mathbb{Z}/p\mathbb{Z}))} p$$

discussed in [3], which has the useful property that, for any integer $n$,

$$\gcd(n, A(E)) = 1 \implies \text{Gal}(\mathbb{Q}(E[n])/\mathbb{Q}) \simeq GL_2(\mathbb{Z}/n\mathbb{Z}).$$

This condition is weaker than (1). For example, if $E$ is the curve $y^2 + y = x^3 - x$, then $A(E) = 30$ and $m_E = 74$. More generally, when $E$ is a Serre curve (for a definition, see [10, pp. 310–311]), one has $A(E) = 30$, whereas $m_E$ is greater than or equal to the square-free part of $|\Delta_E|$.\[1\]

---

[1] By the square-free part $|\Delta_E|$, we mean the unique square-free number $n$ such that $|\Delta_E|/n$ is a square.
Notation 5. For a fixed elliptic curve \( E \) over \( \mathbb{Q} \) and for any positive integer \( n \) we will denote
\[
L_n \coloneq \mathbb{Q}(E[n]), \quad G(n) \coloneq \text{Gal}(L_n/\mathbb{Q}),
\]
and we will regard \( G(n) \) as a subgroup of \( GL_2(\mathbb{Z}/n\mathbb{Z}) \). Also, we will overwork the symbol \( \pi \), using it to denote any one of the canonical projections
\[
\pi : GL_2(\hat{\mathbb{Z}}) \to GL_2(\mathbb{Z}/n\mathbb{Z}), \quad \pi : GL_2(\mathbb{Z}_p) \to GL_2(\mathbb{Z}/p^n\mathbb{Z}),
\]
or \( \pi : GL_2(\mathbb{Z}/n\mathbb{Z}) \to GL_2(\mathbb{Z}/d\mathbb{Z}) \) ( \( d \) dividing \( n \)),
or the restrictions of any of these projections to closed subgroups, for example
\[
\pi : \varphi_E(\text{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})) \to G(M) \quad \text{or} \quad \pi : G(n) \to G(d) \quad (d \text{ dividing } n).
\]

We hope that these abbreviations will minimize cumbersome notation and not cause any confusion. We will say that an integer \( M \) divides \( N^\infty \) if whenever a prime \( p \) divides \( M \), \( p \) also divides \( N \). Throughout, the letters \( p \) and \( \ell \) will always denote prime numbers.

2. Proof of Theorem 3

Let \( E \) be a fixed non-CM elliptic curve over a number field \( K \) and denote by
\[
\varphi_{E,p} : \text{Gal}(\overline{K}/K) \to GL_2(\mathbb{Z}_p) \simeq \text{Aut}(\varprojlim_p E[p^n])
\]
the Galois representation on the Tate module of \( E \) at \( p \). The following is a re-statement of [1, Theorem 1.2].

Theorem 6. Let \( K \) be a number field and let \( p \) be a prime number. There exists an exponent \( n_K(p) \) so that, for each non-CM elliptic curve \( E \) over \( K \), one has
\[
\varphi_{E,p}(\text{Gal}(\overline{K}/K)) = \pi^{-1}(\text{Gal}(K(E[p^{n_K(p)}])/K)).
\]

If \( n_K(p) = 0 \), this is interpreted to mean that \( \varphi_{E,p} \) is surjective. In fact, for \( K = \mathbb{Q} \) and \( p > 3 \) one has
\[
G(p) \simeq GL_2(\mathbb{Z}/p\mathbb{Z}) \quad \Rightarrow \quad n_{\mathbb{Q}}(p) = 0.
\]

This is proved by applying [3, Lemma 3, p. IV-23] with \( X \) equal to the commutator subgroup of \( \varphi_{E,p}(\text{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})) \), together with the fact that thanks to the Weil pairing, the determinant map
\[
\det : \text{Gal}(L_p^\infty/\mathbb{Q}) \to (\mathbb{Z}_p)^*
\]
is surjective, where \( L_p^\infty \coloneq \bigcup_{n=1}^\infty L_{p^n} \). We define
\[
S \coloneq \{2, 3, 5\} \cup \{ p \text{ prime } : G(p) \varsubsetneq GL_2(\mathbb{Z}/p\mathbb{Z}) \text{ or } p \mid \Delta_E\}.
\]

For each prime \( p \in S \), define the exponents
\[
\alpha_p \coloneq \max \{1, \text{ the exponent } n_{\mathbb{Q}}(p) \text{ of Theorem 5}\}
\]
and
\[
\beta_p \coloneq \text{ the exponent of } p \text{ occurring in } GL_2 \left( \mathbb{Z}/\left( \prod_{\ell \in S \setminus \{p\}} \ell \right) \mathbb{Z} \right).
\]

Finally, define the positive integer
\[
n_E \coloneq \prod_{p \in S} p^{\alpha_p + \beta_p}.
\]
Note that, for \( p \in S \) and \( M \) dividing \( (n_E/p^{\alpha_p+\beta_p})^\infty \), one has
\[
\beta_p \geq \text{the exponent of } p \text{ in } |GL_2(\mathbb{Z}/M\mathbb{Z})|.
\]
Using the above definitions and facts, we will prove

**Theorem 7.** Let \( E \) be any elliptic curve defined over \( \mathbb{Q} \). Then
\[
\varphi_E(Gal(\overline{\mathbb{Q}}/\mathbb{Q})) = \pi^{-1}(Gal(\mathbb{Q}(E[n_E])/\mathbb{Q})),
\]
where \( n_E \) is defined in \( (5) \). In particular, \( m_E \leq n_E \).

Note that
\[
\prod_{p \in S} p^{\beta_p} \leq \left| GL_2 \left( \mathbb{Z} / \left( \prod_{\ell \in S} \ell \right) \mathbb{Z} \right) \right| \ll \prod_{\ell \mid \Delta_E} \ell^4,
\]
so that, by \( (1) \) and \( (2) \), if \( E \) is semi-stable and non-CM then
\[
n_E \ll (\prod_{\ell \mid \Delta_E} \ell)^5,
\]
and an affirmative answer to Question \( (2) \) for \( K = \mathbb{Q} \) would imply the above bound for all non-CM elliptic curves \( E \) over \( \mathbb{Q} \). Thus, Theorem 3 is a corollary of Theorem 7.

**Proof of Theorem 7.** First we will prove

**Lemma 8.** For any positive integer \( n_1 \) dividing \( n_E^{\infty} \), one has
\[
G(n_1) = \pi^{-1}(G(d)),
\]
where \( d \) is the greatest common divisor of \( n_1 \) and \( n_E \).

In the language of \( (5) \), this lemma says that \( n_E \) “stabilizes” the Galois representation \( \varphi_E \). The second lemma says that \( n_E \) “splits” \( \varphi_E \) as well.

**Lemma 9.** For any positive integers \( n_1 \) dividing \( n_E^{\infty} \) and \( n_2 \) coprime to \( n_E \), one has
\[
G(n_1n_2) \simeq G(n_1) \times GL_2(\mathbb{Z}/n_2\mathbb{Z}).
\]

The two lemmas together imply Theorem 7. \( \square \)

**Proof of Lemma 8.** Fix an arbitrary divisor \( d \) of \( n_E \). The statement of the lemma is trivial if \( n_1 = d \). Now we will prove it by induction on the set
\[
\mathcal{N}_d := \{ n \in \mathbb{N} : n \text{ divides } n_E^{\infty}, \gcd(n, n_E) = d \}.
\]
Let \( n_1 \in \mathcal{N}_d \) and suppose that for each \( n \in \mathcal{N}_d \cap \{1, 2, \ldots, n_1 - 1\} \), the statement of the lemma is true. Notice that if \( n_1 > d \), then there must exist a prime \( p \in S \) satisfying
\[
p^{\alpha_p+\beta_p} \text{ exactly divides } d \text{ and } p^{\alpha_p+\beta_p+1} \text{ divides } n_1.
\]
Write \( n_1 = p^{r+1}M \), where \( p \) does not divide \( M \) and
\[
r \geq \alpha_p + \beta_p.
\]
We will show that
\[
L_{p^{r+1}} \cap L_{p^r} \cap L_{M}.
\]
If this is true, then, writing \( k \) for this common field, we have that
\[
Gal(L_{p^{r+1}}L_{M}/k) \simeq Gal(L_{p^{r+1}}/k) \times Gal(L_{M}/k)
\]
and

\[
\text{Gal}(L_p, L_M/k) \simeq \text{Gal}(L_{p^r}/k) \times \text{Gal}(L_M/k),
\]
from which it follows that \([L_{p^{r+1}}, M : L_{p^r}M] = [L_{p^r+1} : L_{p^r}]\). Since \(r \geq \alpha_p\), we conclude that

\[
G(n_1) = \pi^{-1}(G(p^r M)),
\]
proving the lemma by induction.

To see why (10) holds, let us write

\[
F_x := L_{p^x} \cap L_M \subseteq L_M \quad (x \geq 1).
\]

Note that, for \(x \geq 1\), the degree \([F_{x+1} : F_x]\) is always a power of \(p\). Thus, if \(\beta_p = 0\), then by (9), we must have \(F_r = F_{r+1}\). Now assume that \(\beta_p \geq 1\). Suppose first that

\[
\forall s \in \{1, 2, \ldots, r - \alpha_p\}, \quad F_{\alpha_p+s-1} \subseteq F_{\alpha_p+s}.
\]

By (10), (8), and (6) we see that this may only happen if \(r = \beta_p + \alpha_p\) and the exponent of \(p\) in \([F_r : \mathbb{Q}]\) is \(\beta_p\). In this case we see from (10) that \(F_{r+1} = F_r\).

Now suppose instead that for some \(s \in \{1, 2, \ldots, r - \alpha_p\}\) one has \(F_{\alpha_p+s-1} = F_{\alpha_p+s}\). We'll first show that under these conditions, \(F_{\alpha_p+s-1} = F_{\alpha_p+s+1}\). To ease notation, we will write \(\alpha := \alpha_p + s - 1\), so that we are trying to prove that

\[
F_{\alpha} = F_{\alpha+1} \implies F_{\alpha} = F_{\alpha+2}.
\]

Denote by

\[
\pi_2 : G(p^{\alpha+2}) \to G(p^{\alpha+1}), \quad \pi_1 : G(p^{\alpha+1}) \to G(p^{\alpha})
\]
the restrictions of the natural projections and let \(N' \subseteq N \subseteq G(p^{\alpha+2})\) be the normal subgroups satisfying

\[
F_\alpha = F_{\alpha+1} = L_{p^{\alpha+2}}^N \quad \text{and} \quad F_{\alpha+2} = L_{p^{\alpha+2}}^{N'}. 
\]

Our contention is that \(N' = N\). Now,

\[
L_{p^{\alpha+2}}^{N'} = L_{p^{\alpha+2}}^N \cap L_{p^{\alpha+2}}^{N'} = L_{p^{\alpha+2}}^N,
\]
which implies that the restriction of \(\pi_2\) to \(N'\) maps surjectively onto \(\pi_2(N)\):

\[
N' \to \pi_2(N).
\]

The fact that \(L_{p^{\alpha+2}}^N = F_\alpha \subseteq L_{p^{\alpha}} = L_{p^{\alpha+2}}^{\ker(\pi_1 \circ \pi_2)}\) implies that

\[
\pi_2^{-1}(\ker \pi_1) = \ker(\pi_1 \circ \pi_2) \subseteq N \subseteq \pi_2^{-1}(\pi_2(N)),
\]
so that

\[
\ker \pi_1 \subseteq \pi_2(N).
\]

Since \(\alpha \geq \alpha_p\), we know that

\[
\ker \pi_2 = I + p^{\alpha+1}M_{2 \times 2}(\mathbb{Z}/p\mathbb{Z}) \quad \text{and} \quad \ker \pi_1 = I + p^{\alpha}M_{2 \times 2}(\mathbb{Z}/p\mathbb{Z}).
\]

Now pick any

\[
I + p^\alpha A \in \ker \pi_1
\]
and find a pre-image \(X = I + p^\alpha A + p^{\alpha+1}B \in N'\). But then

\[
X' = I + p^{\alpha+1}B \mod p^{\alpha+2} \in N',
\]
and so \(I + p^{\alpha+1}M_{2 \times 2}(\mathbb{Z}/p\mathbb{Z}) = \ker \pi_2 \subseteq N'\). This together with (11) shows that \(N' = N\), as desired. Replacing \(s\) by \(s+1\) and repeating the argument inductively, we conclude that \(F_{\alpha_p+s-1} = F_{\alpha_p+k}\) for any positive integer \(k \geq s - 1\), so that in particular \(F_{r+1} = F_r\). This finishes the proof of Lemma 8. \(\square\)
Proof of Lemma [9]. The reasoning here is very similar to that of [5] Theorem 6.1, p. 49]. The first step is to prove

**Sublemma 10.** Fix any integers $M_1$ and $M_2$ with the property that $2 
 M_2$, and $\gcd(M_1 \Delta_E, M_2) = 1$. If $G(M_2) \simeq GL_2(\mathbb{Z}/M_2\mathbb{Z})$, then

$$G(M_1M_2) \simeq G(M_1) \times GL_2(\mathbb{Z}/M_2\mathbb{Z}).$$

Proof of Sublemma [10] Set $F := L_{M_1} \cap L_{M_2}$. We need to show that $F = \mathbb{Q}$. Suppose that $F \neq \mathbb{Q}$. Note that $1 \neq \text{Gal}(F/\mathbb{Q})$ is a common quotient group of $G(M_1)$ and $G(M_2) \simeq GL_2(\mathbb{Z}/M_2\mathbb{Z})$. Replacing $F$ by a subfield, we may assume that $\text{Gal}(F/\mathbb{Q})$ is a common non-trivial simple quotient. We claim that this common simple quotient must be abelian. For a finite group $G$ let $\text{Occ}(G)$ denote the set of simple non-abelian groups which occur as quotients of subgroups of $G$. One easily deduces from [9] p. IV-25] that, for any positive integer $M$, $\text{Occ}(GL_2(\mathbb{Z}/M\mathbb{Z}))$ is equal to

$$\left( \bigcup_{p| M \atop p \equiv 1 \mod 5} \{PSL_2(\mathbb{Z}/p\mathbb{Z}), A_5\} \right) \cup \left( \bigcup_{p| M \atop p \equiv 2 \mod 5} \{PSL_2(\mathbb{Z}/p\mathbb{Z})\} \right) \cup \left( \bigcup_{p| M \atop p = 5} \{A_5\} \right).$$

(Note that $A_5 \simeq PSL_2(\mathbb{Z}/5\mathbb{Z})$.) One can use elementary group theory to show that

$$\{\text{simple non-abelian quotients of } GL_2(\mathbb{Z}/M\mathbb{Z})\} \subseteq \bigcup_{p| M \atop p > 3} \{PSL_2(\mathbb{Z}/p\mathbb{Z})\}.$$ 

Thus, the assumptions on $M_1$ and $M_2$ imply that $\text{Gal}(F/\mathbb{Q})$ must be abelian. Since $M_2$ is odd, the commutator subgroup

$$[GL_2(\mathbb{Z}/M_2\mathbb{Z}), GL_2(\mathbb{Z}/M_2\mathbb{Z})] = SL_2(\mathbb{Z}/M_2\mathbb{Z}),$$

which implies that $F$ is contained in the cyclotomic field

$$F \subseteq \mathbb{Q}\left(\exp\left(\frac{2\pi i}{M_2}\right)\right).$$

Let $p$ be a prime ramified in $F$. We see that $p$ must divide the discriminants of both $L_{M_1}$ and $\mathbb{Q}\left(\exp\left(\frac{2\pi i}{M_2}\right)\right)$, which is impossible since $\gcd(M_1 \Delta_E, M_2) = 1$. Since $\mathbb{Q}$ has no everywhere unramified extensions, we have arrived at a contradiction. Thus, we cannot have $F \neq \mathbb{Q}$, and the sublemma is proved. \qed

To prove Lemma [9] we first prove by induction on the number of primes $p$ dividing $n_2$ that in fact

$$G(n_2) \simeq GL_2(\mathbb{Z}/n_2\mathbb{Z}).$$

The case where $n_2$ is a power of a prime $p > 5$ follows from [11]. Then, (12) is proved by writing $n_2 = p^n M$ with $n \geq 1$ and $p \nmid M$ and by applying Sublemma [10] with $M_1 = p^n$ and $M_2 = M$. Finally, to prove Lemma [9] we apply the sublemma with $M_i = n_i$. \qed

We end by asking the following weakening of Question [2].
Question 11. Fix a number field $K$. Does there exist a constant $C_K$ so that for each prime number $p$ one has

$$n_K(p) \leq C_K,$$

where $n_K(p)$ is the exponent occurring in Theorem 6.

Conditional upon an affirmative answer to this question, Theorem 7 together with [3, Theorem 2] would imply that for any non-CM elliptic curve $E$ over $\mathbb{Q}$, one has

$$m_E \ll \left( \prod_{p \leq B_E} p \right)^{C_0 + 4} \cdot \left( \prod_{p \mid \Delta_E} p \right)^5,$$

where

$$B_E := \frac{4\sqrt{6}}{3} \cdot N_E \prod_{p \mid \Delta_E} \left( 1 + \frac{1}{p} \right)^{1/2} + 1,$$

$N_E$ denoting the conductor of $E$.

ACKNOWLEDGMENTS

I would like to thank C. David and A. C. Cojocaru for stimulating discussions and for comments on an earlier version.

REFERENCES


CENTRE DE RECHERCHES MATHEMATIQUES, UNIVERSITÉ DE MONTRÉAL, P.O. BOX 6128, CENTRE-VILLE STATION, MONTRÉAL, QUÉBEC H3C 3J7, CANADA

E-mail address: Jones@dms.umontreal.ca

License or copyright restrictions may apply to redistribution; see http://www.ams.org/journal-terms-of-use