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 $GL_2(\hat{\mathbb{Z}}) \to GL_2(\mathbb{Z}/mE\mathbb{Z})$. 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 $\text{Aut}(E_{\text{tors}}) \cong GL_2(\hat{\mathbb{Z}})$. 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 $\varphi_E$:
**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
$$\text{Gal}(K(E[p])/K) \simeq \text{GL}_2(\mathbb{Z}/p\mathbb{Z}).$$

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 $\implies \forall p \geq 11$, $\text{Gal}(\mathbb{Q}(E[p])/\mathbb{Q}) \simeq \text{GL}_2(\mathbb{Z}/p\mathbb{Z}).$

His work also shows that, if $p > 19$, $p \not\in \{37, 43, 67, 163\}$, and

(3) $\text{Gal}(\mathbb{Q}(E[p])/\mathbb{Q}) \not\subseteq \text{GL}_2(\mathbb{Z}/p\mathbb{Z}),$

then $\text{Gal}(\mathbb{Q}(E[p])/\mathbb{Q})$ is contained in the normalizer of a Cartan subgroup of $\text{GL}_2(\mathbb{Z}/p\mathbb{Z})$. 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

$A \ll B \iff \exists$ an absolute constant $c$ 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
$$\text{Gal}(\mathbb{Q}/\mathbb{Q}) \to \text{GL}_2(\mathbb{Z}/p\mathbb{Z}),$$

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

$$A(E) := 2 \cdot 3 \cdot 5 \cdot \prod_{p \text{ prime}, p | \Delta_E} p,$$

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

$$\gcd(n, A(E)) = 1 \implies \text{Gal}(\mathbb{Q}(E[n])/\mathbb{Q}) \simeq \text{GL}_2(\mathbb{Z}/n\mathbb{Z}).$$

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 $|\Delta_E|$.\footnote{By the square-free part $|\Delta_E|$, we mean the unique square-free number $n$ such that $|\Delta_E|/n$ is a square.}

License or copyright restrictions may apply to redistribution; see https://www.ams.org/journal-terms-of-use
Notation 5. For a fixed elliptic curve $E$ over $\mathbb{Q}$ and for any positive integer $n$ we will denote

$$L_n := \mathbb{Q}(E[n]), \quad G(n) := \text{Gal}(L_n/\mathbb{Q}),$$

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

$$\pi : GL_2(\mathbb{Z}) \to GL_2(\mathbb{Z}/n\mathbb{Z}), \quad \pi : GL_2(\mathbb{Z}_p) \to GL_2(\mathbb{Z}/p^n\mathbb{Z}),$$

or

$$\pi : GL_2(\mathbb{Z}/n\mathbb{Z}) \to GL_2(\mathbb{Z}/d\mathbb{Z}) \quad (d \text{ dividing } n),$$

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

$$\varphi_{E,p} : \text{Gal}(\overline{K}/K) \to GL_2(\mathbb{Z}_p) \cong \text{Aut}(\lim\limits_{\rightarrow} E[p^n])$$

the Galois representation on the Tate module of $E$ at $p$. The following is a restatement 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

$$G(p) \simeq GL_2(\mathbb{Z}/p\mathbb{Z}) \implies n_\mathbb{Q}(p) = 0. \quad (4)$$

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 $L_{p^\infty} := \bigcup_{n=1}^{\infty} L_{p^n}$. We define

$$S := \{2, 3, 5\} \cup \{p \text{ prime} : G(p) \not\subset GL_2(\mathbb{Z}/p\mathbb{Z}) \text{ or } p \mid \Delta_E\}.$$

For each prime $p \in S$, define the exponents $n_\mathbb{Q}(p)$ of Theorem 5 and

$$\alpha_p := \max \{1, \text{ the exponent } n_\mathbb{Q}(p) \text{ of Theorem 5}\}$$

and

$$\beta_p := \text{ the exponent of } p \text{ occurring in } \left| GL_2\left(\mathbb{Z}/\left(\prod_{\ell \in S\setminus\{p\}} \ell\right)\mathbb{Z}\right) \right|. \quad (5)$$

Finally, define the positive integer

$$n_E := \prod_{p \in S} p^{\alpha_p + \beta_p}.$$
Note that, for $p \in S$ and $M$ dividing $(n_E/p^{\alpha_p+\beta_p})^\infty$, one has
\begin{equation}
\beta_p \geq \text{the exponent of } p \text{ in } |GL_2(\mathbb{Z}/MZ)|.
\end{equation}

Using the above definitions and facts, we will prove

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

Note that
\[ \prod_{p \in S} p^{\beta_p} \leq \left| GL_2 \left( \mathbb{Z}/ \left( \prod_{\ell \in S} \ell \right) \mathbb{Z} \right) \right| \ll \prod_{\ell \in S} \ell^4, \]
so that, by (4) and (2), if $E$ is semi-stable and non-CM then
\begin{equation}
(7) \quad n_E \ll \left( \prod_{\ell | \Delta_E} \ell \right)^5,
\end{equation}
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
\[ G(n_1 n_2) \simeq G(n_1) \times GL_2(\mathbb{Z}/n_2 \mathbb{Z}). \]

The two lemmas together imply Theorem 7. □

**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
\begin{equation}
r \geq \alpha_p + \beta_p.
\end{equation}
We will show that
\begin{equation}
L_{p^{r+1} \cap M} = L_{p^r \cap M}.
\end{equation}
If this is true, then, writing $k$ for this common field, we have that
\[ \text{Gal} \left( L_{p^{r+1} \cap M}/k \right) \simeq \text{Gal} \left( L_{p^{r+1}}/k \right) \times \text{Gal} \left( L_M/k \right) \]
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 \([L_{p^{r+1}} : L_p] = [L_{p^{r+1}} : L_p^r].\) 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 (9) holds, let us write
(10) \[ F_x := L_{p^r} \cap L_M \subseteq L_M \quad (x \geq 1). \]
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
\[ F_\alpha = F_{\alpha+1} = L_{p^\alpha}^{N'} \quad \text{and} \quad F_{\alpha+2} = L_{p^\alpha}^{N'}. \]
Our contention is that \(N' = N.\) Now,
(11) \[ L_{p^\alpha}^{\ker \pi_2 N'} = L_{p^\alpha}^{\ker \pi_2} \cap L_{p^\alpha}^{N'} = L_{p^\alpha}^N, \]
which implies that the restriction of \(\pi_2\) to \(N'\) maps surjectively onto \(\pi_2(N):\)
\[ N' \twoheadrightarrow \pi_2(N). \]
The fact that \(L_{p^\alpha}^N = F_\alpha \subseteq L_{p^\alpha} = L_{p^\alpha}^{\ker(\pi_1 \circ \pi_2)}\) 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
\[ X' \equiv I + p^{\alpha+1}A \mod p^{\alpha+2} \in N', \]
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 \(F_{\alpha_p + s - 1} = F_{\alpha_p + s}\) 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 $2 
mid M_2$, $5 
mid M_2$, 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

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

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

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

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. \hfill \Box

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 $n_2 = p^k M$ with $n \geq 1$ and $p \nmid M$ and by applying Sublemma 10 with $M_1 = p^k$ and $M_2 = M$. Finally, to prove Lemma 9 we apply the sublemma with $M_1 = n_1$. \hfill \Box

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

$$m_E \ll \left( \prod_{p \leq B_E} p \right)^{c_0 + 4} \cdot \left( \prod_{p|\Delta_E} p \right)^5,$$

where

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

$N_E$ 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

[1] K. Arai, On uniform lower bound of the Galois images associated to elliptic curves, preprint (2007). Available at http://arxiv.org/abs/math/0703686.

[2] I. Chen, The Jacobians of non-split Cartan modular curves, Proc. London Math. Soc. (3) 77, no. 1 (1998), 1–38. MR1625491 (99m:11068)

[3] A. C. Cojocaru, On the surjectivity of the Galois representations associated to non-CM elliptic curves, with an appendix by Ernst Kani, Canad. Math. Bull. 48 (2005), no. 1, 16–31. MR2118760 (2005k:11109)

[4] A. Kraus, Une remarque sur les points de torsion des courbes elliptiques, C. R. Math. Acad. Sci. Paris, 321, Série I (1995), 1143–1146. MR1360773 (97a:11085)

[5] S. Lang and H. Trotter, Probenien distributions in GL2-extensions, Lecture Notes in Math., 504, Springer-Verlag, Berlin, 1976. MR0568299 (81j:12004)

[6] D. Masser and G. Wüstholz, Galois properties of division fields of elliptic curves, Bull. London Math. Soc. 25 (1993), 247–254. MR1209248 (94d:11036)

[7] B. Mazur, Rational isogenies of prime degree, Invent. Math. 44, no. 2 (1978), 129–162. MR482230 (80h:14022)

[8] P. E. Parent, Towards the triviality of $X_0^+(p^r)(\mathbb{Q})$ for $r > 1$, Compos. Math. 141, no. 3 (2005), 561–572. MR2135276 (2006a:11076)

[9] J-P. Serre, Abelian l-adic representations and elliptic curves, Benjamin, New York-Amsterdam, 1968. MR0268166 (42:2292)

[10] , Propréties galoisiennes des points d’ordre fini des courbes elliptiques, Invent. Math. 15 (1972), 259–331. MR0387283 (52:8126)

[11] , Quelques applications du théorème de densité de Chebotarev, Inst. Hautes Études Sci. Publ. Math. 54 (1981), 123–201 (323–401). MR644559 (83k:12011)

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

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