

Merel's theorem on the boundedness of the torsion of elliptic curves

Marusia Rebolledo

ABSTRACT. In this note, we give the key steps of Merel's proof of the Strong Uniform Boundedness Conjecture. This proof relies on three fundamental ingredients: the geometric approach of Mazur and Kamienny, the innovative introduction of the winding quotient by Merel, and the use of Manin's presentation of the homology group of modular curves.

1. Introduction

Interest in elliptic curves dates back at least to Fermat, who introduced his fundamental method of infinite descent to prove his "Last Theorem" in degree 4. Poincaré seems to have been the first to conjecture, around 1901, the now famous theorem of Mordell asserting that the group of rational points of an elliptic curve over \mathbb{Q} is finitely generated. This result was later generalized by Weil to encompass all abelian varieties over number fields. If E is an elliptic curve over a number field K , it is therefore known that

$$E(K) \cong \mathbb{Z}^r \oplus T$$

as abstract groups, where $T = E(K)_{\text{tors}}$ is the finite *torsion subgroup* of $E(K)$. The integer r , called the rank, is a subtle invariant about which little is known and which can be rather hard to compute given E and K . The torsion subgroup, in contrast, is readily computed in specific instances, and this makes it realistic to ask more ambitious questions about the variation of $E(K)_{\text{tors}}$ with E and K . A fundamental result in this direction is the theorem of Mazur presented in Chapter 3 of Darmon's lecture in this volume, which gives a uniform bound on $E(\mathbb{Q})_{\text{tors}}$ as E varies over all elliptic curves over \mathbb{Q} . Kamienny [Kam92] was able to extend Mazur's result to quadratic fields, obtaining a bound on $E(K)_{\text{tors}}$ for K quadratic that was even independent of K itself. This led him to formulate the Strong Uniform Boundedness Conjecture, asserting that the cardinality of $E(K)_{\text{tors}}$ can be bounded above by a constant which depends only on the degree of K/\mathbb{Q} . (The weaker conjecture asserting that the torsion can be bounded uniformly in the field K is presented as being 'a part of the folklore' by Cassels [Cas66] (p. 264).) Actually, according to Demjanenko (see [Dem72] and entry MR0302654 in Mathematical Reviews) this

2000 *Mathematics Subject Classification*. Primary 11G05.

conjecture was posed in the 70's by Shafarevich; his paper proved a result in this direction. The Strong Uniform Boundedness Conjecture was proved in 1994 by Merel, building on the methods developed by Mazur and Kamienny.

THEOREM 1 (Merel 1994). *For all $d \in \mathbb{Z}$, $d \geq 1$ there exists a constant $B(d) \geq 0$ such that for all elliptic curves E over a number field K with $[K : \mathbb{Q}] = d$ then*

$$|E(K)_{\text{tors}}| \leq B(d).$$

Merel actually proved the following bound on the prime numbers dividing $E(K)_{\text{tors}}$:

THEOREM 2 (Merel - 1994). *Let E be an elliptic curve over a number field K such that $[K : \mathbb{Q}] = d > 1$. Let p be a prime number. If $E(K)$ has a p -torsion point then $p < d^{3d^2}$.*

It is then sufficient to conclude for the case $d > 1$. Mazur and Kamienny [KM95] have indeed shown that, by work of Faltings and Frey, Theorem 2 implies Theorem 1. The case $d = 1$ of Theorem 1 has been proved by Mazur [Maz77, Maz78] in 1976 as explained by Henri Darmon in his lecture. Mazur gives more precisely a list of all possibilities for the torsion group over \mathbb{Q} . It was actually a conjecture of Levi formulated around 1908. We can mention also that the cases $2 \leq d \leq 8$ and $9 \leq d \leq 14$ have been treated respectively by Kamienny and Mazur (see [KM95]), and Abramovich [Abr95].

The goal of this note is to give the key steps of the proof of Theorem 2.

REMARK 1. Oesterlé [Oes] later improved the bound of Theorem 2 to $(3^{d/2} + 1)^2$ but we will focus on Merel's original proof (see Section 3.6 concerning Oesterlé's trick).

REMARK 2. Unfortunately, the reduction of Theorem 1 to Theorem 2 is not effective; this explains why the global bound $B(d)$ is not explicit. However, in 1999, Parent [Par99] gave a bound for the p^r -torsion ($r \geq 1, p$ prime) and thus obtained a global effective bound for the torsion (later improved by Oesterlé). This bound is exponential in d . It is conjectured that $B(d)$ can be made polynomial in d .

We will now give the sketch of the proof of Theorem 2. From now on, we will denote by $d \geq 1$, an integer, by p a prime number and write $Z = \mathbb{Z}[1/p]$. Following the traditional approach, Mazur and Kamienny translated the assertion of the theorem into an assertion about rational points of some modular curves.

2. Mazur's method

2.1. To a problem on modular curves. We briefly recall that there exist smooth schemes $X_0(p)$ and $X_1(p)$ over Z which classify, coarsely and finely respectively, the generalized elliptic curves endowed with a subgroup, respectively a point, of order p . We refer for instance to Chapter 3 of [Dar] for more details. We denote by $Y_0(p)$ and $Y_1(p)$ the respective affine parts of $X_0(p)$ and $X_1(p)$. We use the subscript \mathbb{Q} for the algebraic curves over \mathbb{Q} obtained by taking the generic fiber of $X_0(p)$ or $X_1(p)$. We will denote by $J_0(p)$ the Néron model over Z of the Jacobian $J_0(p)_{\mathbb{Q}}$ of $X_0(p)_{\mathbb{Q}}$.

Suppose that E is an elliptic curve over a number field K of degree $d \geq 1$ over \mathbb{Q} , endowed with a K -rational p -torsion point P . Then (E, P) defines a point

$\tilde{x} \in Y_1(p)(K)$. We can map this point to a point $x \in Y_0(p)(K)$ through the usual covering $X_1(p) \rightarrow X_0(p)$.

If we denote by v_1, \dots, v_d the embeddings of K into \mathbb{C} , we then obtain a point $\underline{x} = (v_1(x), \dots, v_d(x)) \in X_0(p)^{(d)}(\mathbb{Q})$. Here we denote by $X_0(p)^{(d)}$ the d -th symmetric power of $X_0(p)$, that is to say the quotient scheme of $X_0(p)$ by the action of the permutation group Σ_d . It is a smooth scheme over Z .

2.2. The Mazur and Kamienny strategy. The strategy is almost the same as in the case $d = 1$ explained in [Dar] Ch.3. Let $A_{\mathbb{Q}}$ denote an abelian variety quotient of $J_0(p)_{\mathbb{Q}}$ and A its Néron model over Z . Kamienny's idea is to approach the Uniform Boundedness Conjecture by studying the natural morphism

$$\phi_A^{(d)} : X_0(p)^{(d)} \xrightarrow{\phi^{(d)}} J_0(p) \rightarrow A$$

defined as follows. Over \mathbb{Q} , this morphism is defined as the composition of the Albanese morphism $(Q_1, \dots, Q_d) \mapsto [(Q_1) + \dots + (Q_d) - d(\infty)]$ with the surjection of $J_0(p)_{\mathbb{Q}}$ to $A_{\mathbb{Q}}$. It then extends to a morphism from the smooth Z -scheme $X_0(p)^{(d)}$ to A . For any prime number $l \neq p$, we denote by $\phi_{A, \mathbb{F}_l}^{(d)} : X_0(p)_{\mathbb{F}_l}^{(d)} \rightarrow A_{\mathbb{F}_l}$ the morphism obtained by taking the special fibers at l . Just as in the case $d = 1$, we have

THEOREM 3 (Mazur-Kamienny). *Suppose that*

- (1) $A(\mathbb{Q})$ is finite;
- (2) there exists a prime number $l > 2$ such that $p > (1 + l^{d/2})^2$ and $\phi_{A, \mathbb{F}_l}^{(d)}$ is a formal immersion at $\infty_{\mathbb{F}_l}^{(d)}$.

Then $Y_1(p)(K)$ is empty for all number fields K of degree d over \mathbb{Q} , i.e., there does not exist any elliptic curve with a point of order p over any number field of degree d .

PROOF. The proof of this theorem is analogous to the one in the case $d = 1$. The principal ingredients of the proof are explained in [Dar] Ch. 3. For a complete proof, the reader can see [Maz78], [Kam92] or, for a summary, [Edi95]. The idea is the following: suppose that there exists a number field K of degree d and a point of $Y_1(p)(K)$ and consider the point $\underline{x} \in X_0(p)^{(d)}(\mathbb{Q})$ obtained as explained in Section 2.1. The condition $p > (1 + l^{d/2})^2$ of Theorem 3 implies that the section s of $X_0(p)^{(d)}$ corresponding to \underline{x} crosses $\infty^{(d)}$ in the fiber at l . Since $s \neq \infty^{(d)}$, the fact that $\phi_{A, \mathbb{F}_l}^{(d)}$ is a formal immersion at $\infty_{\mathbb{F}_l}^{(d)}$ and Condition 1 will then give a contradiction. □

We now need an abelian variety $A_{\mathbb{Q}}$ quotient of $J_0(p)_{\mathbb{Q}}$ of rank 0 (see section 3.1) and a formal immersion criterion (see below).

2.3. Criterion of formal immersion. Recall first that a morphism $\phi : X \rightarrow Y$ of noetherian schemes is a *formal immersion* at a point $x \in X$ which maps to $y \in Y$ if the induced morphism on the formal completed local rings $\hat{\phi} : \widehat{\mathcal{O}_{Y, y}} \rightarrow \widehat{\mathcal{O}_{X, x}}$ is surjective. Equivalently, it follows from Nakayama's lemma that ϕ is a formal immersion at x if the two following conditions hold:

- (1) the morphism induced on the residue fields $k(y) \rightarrow k(x)$ is an isomorphism;