HAL open science

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

Marusia Rebolledo

To cite this version:

Marusia Rebolledo. Merel's theorem on the boundedness of the torsion of elliptic curves. Arithmetic geometry, American Mathematical Society, pp.71-82, 2009. hal-00483912

HAL Id: hal-00483912

https://hal.science/hal-00483912v1

Submitted on 17 May 2010

HAL is a multi-disciplinary open access archive for the deposit and dissemination of scientific research documents, whether they are published or not. The documents may come from teaching and research institutions in France or abroad, or from public or private research centers.

L'archive ouverte pluridisciplinaire **HAL**, est destinée au dépôt et à la diffusion de documents scientifiques de niveau recherche, publiés ou non, émanant des établissements d'enseignement et de recherche français ou étrangers, des laboratoires publics ou privés.

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

Marusia Rebolledo

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[1] of $K/\mathbb{Q}$. Actually, Demjanenko claimed that this conjecture would have been set out already in the 70's by Shafarevich and proved in 1972 a result in this direction (see [Dem72] and the mathematical review MR0302654). The Strong Uniform Boundedness Conjecture was proved in 1994 by Merel, building on the methods developped 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*

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

[1] The weaker conjecture asserting that the torsion can be bounded uniformly in the field K is presented as beeing " a part of the folklore" by Cassels [Cas66] (p. 264).

Merel actually proves 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 showed that, by Faltings and Frey works, Theorem 2 implies Theorem 1. The case $d = 1$ of Theorem 1 has been proved by Mazur [Maz77, Maz78] in 1976 as explained 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 by $(3^{d/2} + 1)^2$ but we will focus on Merel's original proof (see Section 3.6 concerning the 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 by $Z = \mathbb{Z}[1/p]$. 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 respectively coarsely and finely 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 $X_1(p) \longrightarrow X_0(p)$.

If we denote by $v_1, \ldots, v_d$ the embeddings of K into $\mathbb{C}$, we then obtain a point $\underline{x} = (v_1(x), \ldots, v_d(x)) \in X_0(p)^{(d)}(\mathbb{Q})$. 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

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

defined as follows. Over $\mathbb{Q}$, this morphism is defined as the composition of the Albanese morphism $(Q_1, \ldots, Q_d) \mapsto [(Q_1) + \ldots (Q_d) - d(\infty)]$ 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 $\phi_{A,\mathbb{F}_l}^{(d)} : X_0(p)_{\mathbb{F}_l}^{(d)} \longrightarrow A_{\mathbb{F}_l}$ 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 $\phi : X \longrightarrow Y$ 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 $\hat{\phi} : \widehat{\mathcal{O}_{Y,y}} \longrightarrow \widehat{\mathcal{O}_{X,x}}$ 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 $k(y) \longrightarrow k(x)$ is an isomorphism;
2. the morphism $\phi^* : \mathrm{Cot}_y(Y) \longrightarrow \mathrm{Cot}_x(X)$ is surjective.

The first condition is verified in our situation, so we are now looking for a criterion to have

$$\phi^{(d)}_{A,\mathbb{F}_l}{}^{*} : \mathrm{Cot}(A_{\mathbb{F}_l}) \longrightarrow \mathrm{Cot}_{\infty^{(d)}_{\mathbb{F}_l}}(X_0(p)^{(d)}_{\mathbb{F}_l})$$

surjective. For this, we will look in more details at $\phi^{(d)}_A{}^{*}$.

Let R be a Z-algebra. As in [dar], denote by $\mathrm{S}_2(\Gamma_0(p), R)$ the regular differentials on $X_0(p)_R = X_0(p) \times_Z R$. For $R = \mathbb{C}$, we obtain the vector space of classical modular forms $\mathrm{S}_2(\Gamma_0(p), \mathbb{C})$. The *q-expansion principle* gives an injective morphism of R-modules

$$\mathrm{S}_2(\Gamma_0(p), R) \hookrightarrow R[[q]].$$

Furthermore, we have an isomorphism between $\mathrm{Cot}(J_0(p)(\mathbb{C}))$ and $\mathrm{S}_2(\Gamma_0(p), \mathbb{C})$ coming from the composition of

1. the isomorphism $H^0(J_0(p)(\mathbb{C}), \Omega^1) \longrightarrow \mathrm{Cot}(J_0(p)(\mathbb{C}))$ which maps a differential form to its evaluation at 0 ;
2. the isomorphism $H^0(J_0(p)(\mathbb{C}), \Omega^1) \xrightarrow{\phi^*} H^0(X_0(p)(\mathbb{C}), \Omega^1) = \mathrm{S}_2(\Gamma_0(p), \mathbb{C})$ given by Serre duality.

It is a non trivial fact that this isomorphism $\mathrm{Cot}(J_0(p)(\mathbb{C})) \cong \mathrm{S}_2(\Gamma_0(p), \mathbb{C})$ extends to an isomorphism over Z (and actually even over $\mathbb{Z}$). Indeed, Grothendieck duality can be applied in this setting instead of Serre duality and we then obtain an isomorphism: $\mathrm{Cot}(J_0(p)) \cong \mathrm{S}_2(\Gamma_0(p), Z)$ (see [Maz78] 2 e)).

On the other hand, we have to understand the cotangent bundle $\mathrm{Cot}_{\infty^{(d)}}(X_0(p)^{(d)})$. Recall that q is a formal local parameter of $X_0(p)$ at ∞ *i.e.* $\widehat{\mathcal{O}}_{X_0(p),\infty} \cong Z[[q]]$. We then have

$$\widehat{\mathcal{O}}_{X_0(p)^{(d)},(\infty)^{(d)}} \cong Z[[q_1, \ldots, q_d]]^{\Sigma_d} = Z[[\sigma_1, \ldots, \sigma_d]]$$

where for $i = 1, \ldots, d$, q_i is a local parameter at ∞ on the ith factor of $X_0(p)^d$ and $\sigma_1 = q_1 + \cdots + q_d, \ldots, \sigma_d = q_1 \ldots q_d$ are the symmetric functions in $q_1, \ldots, q_d$. Consequently, $\mathrm{Cot}_{\infty^{(d)}}(X_0(p)^{(d)})$ is a free Z-module of rank d with a basis given by the differential forms $(d\sigma_1, \ldots, d\sigma_d)$.

We obtain the following diagram:

$$\begin{tikzcd}
\mathrm{Cot}(J_0(p)) \arrow[r, "\phi^*", "\sim"'] \arrow[d, "\phi^{(d)*}"] & \mathrm{S}_2(\Gamma_0(p), Z) \arrow[r, hook, "q-exp"] & Z[[q]] \\
\mathrm{Cot}(X_0(p)^{(d)}) & &
\end{tikzcd}$$

Lemma 1. *Let $\omega \in \mathrm{Cot}(J_0(p))$ be such that $\phi^*(\omega)$ has a q-expansion equal to $\sum_{m\geq 1} a_m q^m \frac{dq}{q}$. Then we have*

$$\phi^{(d)*}(\omega) = a_1 d\sigma_1 - a_2 d\sigma_2 + \cdots + (-1)^{d-1} a_d d\sigma_d.$$

Proof. Denote by $\pi : X_0(p)^d \longrightarrow X_0(p)^{(d)}$ the canonical map. We have

$$\pi^* \phi^{(d)*}(\omega) = \sum_{i=1}^{d} \sum_{m\geq 1} a_m q_i^m \frac{dq_i}{q_i} = \sum_{m\geq 1} a_m m^{-1} ds_m$$

where $s_m = \sum_{i=1}^{d} q_i^m$. Then Newton's formula

$$s_m - \sigma_1 s_{m-1} + \cdots + (-1)^m m\sigma_m = 0$$

gives $m^{-1} ds_m = (-1)^m d\sigma_m$ for $m \in \{1, \ldots, d\}$. □

We suppose in the sequel that $A_{\mathbb{Q}}$ is the quotient of $J_0(p)_{\mathbb{Q}}$ by an ideal I of the *Hecke algebra* $\mathbb{T} \subset \mathrm{End}(J_0(p)_{\mathbb{Q}})$, so that there is an induced action of $\mathbb{T}$ on A. The exact sequence

$$0 \to IJ_0(p)_{\mathbb{Q}} \to J_0(p)_{\mathbb{Q}} \to A_{\mathbb{Q}} \to 0$$

induces a reverse exact sequence for the cotangent bundles after scalar extension by $Z[1/2]$

$$0 \to \mathrm{Cot}(A_{Z[1/2]}) \to \mathrm{Cot}(J_0(p)_{Z[1/2]}) \to \mathrm{Cot}(J_0(p)_{Z[1/2]})[I] \to 0$$

where we denote by $\mathrm{Cot}(J_0(p)_{Z[1/2]})[I]$ the differential forms annihilated by I. This is due to a *specialization lemma* of Raynaud (see [Maz78] Proposition 1.1 and Corollary 1.1).

Let $l \neq 2, p$ be a prime number. We finally have the following diagram in characteristic l:

$$\begin{tikzcd}
\mathrm{Cot}(A_{\mathbb{F}_l}) \arrow[r, hook] \arrow[dr, "\phi^{(d)*}_{A,\mathbb{F}_l}"'] & \mathrm{Cot}(J_0(p)_{\mathbb{F}_l}) \arrow[r, "\phi^*_{\mathbb{F}_l}", "\sim"'] \arrow[d, "\phi^{(d)*}_{\mathbb{F}_l}"] & \mathrm{S}_2(\Gamma_0(p), \mathbb{F}_l) \arrow[r, hook, "q-exp"] & \mathbb{F}_l[[q]] \\
& \mathrm{Cot}_{\infty^{(d)}_{\mathbb{F}_l}}(X_0(p)^{(d)}_{\mathbb{F}_l}) & &
\end{tikzcd}$$

This diagram and Lemma 1 give a criterion for $\phi^{(d)}_{A,\mathbb{F}_l}$ to be a formal immersion at $\infty^{(d)}_{\mathbb{F}_l}$ (see Theorem 5 below). Historically, Mazur first showed the following result which completes the proof of Mazur's theorem sketched in Section 4 of [dar] using for $A_{\mathbb{Q}}$ the *Eisenstein quotient*.

Theorem 4. *Let $A_{\mathbb{Q}}$ be the quotient of $J_0(p)_{\mathbb{Q}}$ by an ideal I of $\mathbb{T}$. The morphism $\phi_{A,\mathbb{F}_l}$ is a formal immersion at $\infty_{\mathbb{F}_l}$ for all prime numbers $l \neq 2, p$.*

Proof. There is a non zero element $\omega \in \mathrm{Cot}(A_{\mathbb{F}_l})$ such that $\phi^*_{\mathbb{F}_l}(\omega) \in \mathrm{S}_2(\Gamma_0(p), \mathbb{F}_l)$ is an eigenform (under the action of the Hecke algebra $\mathbb{T}$). Then by the q-expansion principle and the injectivities in the above diagram, its q-expansion is not identically zero (because if it was, $\phi^*_{\mathbb{F}_l}(\omega)$ itself would be zero). We deduce that $a_1(\omega) \neq 0$: indeed, if it was, since ω is an eigenform, we should have $a_m(\omega) = a_1(T_m\omega) = \lambda_m(\omega)a_1(\omega) = 0$ for all $m \geq 1$, so $\omega = 0$, which is impossible. It follows that $a_1(\omega)$ spans $\mathrm{Cot}_{\infty_{\mathbb{F}_l}}(X_0(p)_{\mathbb{F}_l}) \cong \mathbb{F}_l$ and, by Lemma 1, that $\phi_{A,\mathbb{F}_l}$ is a formal immersion at $\infty_{\mathbb{F}_l}$. □

Theorem 5 (Kamienny). *The following assertions are equivalent:*

1. *$\phi^{(d)}_{A,\mathbb{F}_l}$ is a formal immersion at $\infty^{(d)}_{\mathbb{F}_l}$;*
2. *there exists d weight-two cusp forms $f_1, \ldots, f_d$ annihilated by I such that the vectors $(a_1(f_i), \ldots, a_d(f_i))_{i=1,\ldots,d}$ are linearly independent mod l;*
3. *the images of $T_1, \ldots, T_d$ in $\mathbb{T}/(l\mathbb{T} + I)$ are $\mathbb{F}_l$-linearly independent.*

Proof. The equivalence of 1. and 2. follows directly from Lemma 1 since $\mathrm{Cot}(A)$ maps to the forms annihilated by I via the isomorphism ϕ^*. Condition 3. is dual to Condition 2. Indeed, the multiplicity one theorem implies that the pairing

$$\begin{array}{rccc} <,>: & \mathrm{S}_2(\Gamma_0(p), \mathbb{Z}) \times \mathbb{T} & \longrightarrow & \mathbb{Z} \\ & (f, t) & \longmapsto & a_1(tf) \end{array}$$

is perfect and then induces an isomorphism of $\mathbb{T}$-modules between $\mathrm{S}_2(\Gamma_0(p), \mathbb{Z})$ and the $\mathbb{Z}$-dual of $\mathbb{T}$. For a more detailed proof of this theorem, see [Kam92] or [Oes] Sections 3, 4 and 6. □

3 Merel's proof

3.1 The Winding Quotient

Denote by $J_{e,\mathbb{Q}}$ the *winding quotient* (see [dar] Ch. 3) and J_e its Néron model over Z. We just recall that $J_{e,\mathbb{Q}}$ is the abelian variety quotient of $J_0(p)_{\mathbb{Q}}$ by the *winding ideal* I_e of $\mathbb{T}$.

Considering Theorem 3, we are now looking for a quotient $A_{\mathbb{Q}}$ of $J_0(p)_{\mathbb{Q}}$ by an ideal $I \subset \mathbb{T}$ such that $A(\mathbb{Q})$ is finite. Mazur and Kamienny have used the *Eisenstein quotient* which has this property (see [Maz77, Kam92]). Merel's fundamental innovation has been to use the winding quotient: this quotient

is greater and easier to exploit than the Eisenstein quotient. This has been made possible after the works of Kolyvagin on the Birch and Swinnerton-Dyer conjecture: indeed, it then turned out that $J_e(\mathbb{Q})$ is finite by construction (see [Mer96] or [dar] for a summary). Actually, the Birch and Swinnerton-Dyer conjecture predicts that the winding quotient is the greatest quotient of $J_0(p)_{\mathbb{Q}}$ of rank zero.

Finally, to prove Theorem 2, thanks to Theorems 3 and 5, it suffices to determine for which prime numbers p the following is true for a prime number $l \neq 2$ such that $p > (1 + l^{d/2})^2$:

$(\star_l)$ the images of $T_1, \ldots, T_d$ in $\mathbb{T}/(l\mathbb{T} + I_e)$ are $\mathbb{F}_l$-linearly independent.

3.2 Merel's strategy

Suppose now that $d \geq 3$. Recall that the Hecke algebra $\mathbb{T} \subset \mathrm{End}(J_0(p))$ also acts on the first group of absolute singular homology $H_1(X;\mathbb{Z})$ of the compact Riemann surface $X = X_0(p)(\mathbb{C})$ and that I_e is the annihilator of the *winding element* $e \in H_1(X;\mathbb{Q})$ (see the article of Darmon in this volume). Then $\mathbb{T}.e$ is a free $\mathbb{T}/I_e$-module of rank 1. It follows that $(\star_l)$ is equivalent to

$(\star_l)$ the images of $T_1e, \ldots, T_de$ in $\mathbb{T}e/l\mathbb{T}e$ are $\mathbb{F}_l$-linearly independent.

As before, the characteristic zero analogous condition

$(\star)$ $T_1e, \ldots, T_de$ are Z-linearly independent in $\mathbb{T}.e$.

is equivalent for $\phi_{I_e}^{(d)}$ to be a formal immersion at $\infty_{\mathbb{Q}}^{(d)}$. If $(\star_l)$ is true for a prime number l then $(\star)$ is true, while the condition $(\star)$ implies $(\star_l)$ for almost all prime number l. Kamienny showed that if $(\star)$ is true then there exists a prime number $l < 2(d!)^{5/2}$ (depending on p) such that $(\star_l)$ is true (see [Kam92] Corollary 3.4 and [Edi95] 4.3 for the precise bound). The heart of the Merel's proof for the boundedness of the torsion of elliptic curve is then to prove $(\star)$ for $p > d^{3d^2} > 2^{d+1}(d!)^{5d/2} \geq (1 + (2(d!)^{5/2})^{d/2})^2$.

We will now explain the key steps of this proof omitting the details of the calculus. For a completed proof, we will refer to [Mer96].

Consider a fixed prime number $p > d^{3d^2}$ for $d \geq 3$ an integer. To prove that $e, T_2e, \ldots, T_de$ are linearly independent, it suffices to prove that so do $e, t_2e, \ldots, t_de$ where $t_r = T_r - \sigma'(r)$ with $\sigma'(r)$ the sum of divisors of r coprime to p. Those slight different Hecke operators t_r are more pleasant to work with because they annihilate the "Eisenstein part" of e and we can then work as if e was equal to the *modular symbol* $\{0, \infty\}$ (see the section 3.3 for a definition)[2].

The idea of the proof is to use the intersection product

$$\bullet : H_1(X;\mathbb{Z}) \times H_1(X;\mathbb{Z}) \longrightarrow \mathbb{Z}.$$

[2]In the relative homology group, the winding element e differs from $\{0, \infty\}$ by an element which is an eigenvector for all T_n with system of eigenvalues $\{\sigma'(n)\}_{n\geq 1}$ (up to a constant): this is what I called the *Eisenstein part*.

Suppose indeed that $\lambda_1 e + \lambda_1 t_2 e + \cdots + \lambda_c t_c e = 0$ for $1 \leq c \leq d$ and some $\lambda_1, \ldots, \lambda_c$ in $\mathbb{Z}$ with $\lambda_c \neq 0$. The strategy is then to find $x_c \in H_1(X;\mathbb{Z})$ such that

$$i)\ t_c e \bullet x_c \neq 0 \qquad \text{and} \qquad ii)\ t_r e \bullet x_c = 0 \quad (1 \leq r \leq c-1).$$

This will give a contradiction.[3]

Two key facts make it possible to follow this strategy: first, there is a presentation of $H_1(X;\mathbb{Z})$ by generators and relations due to Manin [Man72] (see the section 3.3); secondly, some lemma called *lemme des cordes* by Merel (Proposition 1 below) enables us to compute the intersection product of two such generators. It suffices then to express $t_r e$ in terms of the Manin's generators (see 3.4).

3.3 Manin's symbols

Denote by $\mathfrak{H}$ the Poincaré upper half plane. For $\alpha, \beta \in \mathbb{P}^1(\mathbb{Q})$, consider the image in $\Gamma_0(p)\backslash\mathfrak{H}$ of the geodesic path from α to β in $\mathfrak{H}$. Denote by $\{\alpha, \beta\}$ its homology class in the homology group $H_1(X, cusps; \mathbb{Z})$ relative to the set *cusps* of the cusps of X.

Exercise 1. *1. Show that $\{\alpha, \beta\}$ is the sum of classes of type $\{b/d, a/c\}$ with $a, b, c, d \in \mathbb{Z}$ such that $ad - bc = 1$ (hint: use continued fractions).*

2. Show that $\{b/d, a/c\}$ depends only on the coset $\Gamma_0(p)\left(\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right)$.

For a solution of this exercise, see [Man72] for instance.

The preceding results imply that there is a surjective map

$$\begin{array}{rccl} \xi\ :\ & \mathbb{Z}[\Gamma_0(p)\backslash \mathrm{SL}_2(\mathbb{Z})] & \longrightarrow & H_1(X, cusps; \mathbb{Z}) \\ & \Gamma_0(p).g & \longmapsto & \{g.0, g.\infty\} = \{\frac{b}{d}, \frac{a}{c}\} \quad g = \left(\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right) \in \mathrm{SL}_2(\mathbb{Z}). \end{array}$$

Since there is moreover an isomorphism

$$\begin{array}{ccc} \Gamma_0(p)\backslash \mathrm{SL}_2(\mathbb{Z}) & \longrightarrow & \mathbb{P}^1(\mathbb{F}_p) \\ \Gamma_0(p).\left(\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right) & \mapsto & [c:d], \end{array}$$

we will simply write $\xi(c/d) := \xi(\left(\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right))$.

For $k \in \mathbb{F}_p^\times$ we obtain $\xi(k) = \{0, 1/k\}$ which is an element of $H_1(X;\mathbb{Z})$ (seen as a submodule of $H_1(X, cusps; \mathbb{Z})$) because 0 and $1/k$ are conjugated modulo $\Gamma_0(p)$. Those elements are generators of $H_1(X;\mathbb{Z})$. The other generators of $H_1(X, cusps; \mathbb{Z})$ are $\xi(0)$ and $\xi(\infty)$ and they verify $\xi(0) = -\xi(\infty) = \{0, \infty\}$.

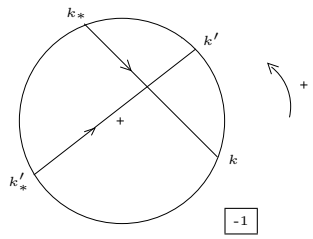
The following proposition, called *lemme des cordes* by Merel, gives a method to compute the intersection product of two Manin symbols in the absolute homology group. For $k \in \{1, \ldots, p-1\}$, denote by k_* the element of $\{1, \ldots, p-1\}$ such that $kk_* \equiv -1 \pmod{p}$.

[3] Actually, for $c = 1$ the situation will be slightly different because of the Eisenstein part of e.

Proposition 1 (Merel). *Let $k, k' \in \{1, \dots, p-1\}$. Denote by C_k the corde of the unit circle from $e^{2i\pi k_*/p}$ to $e^{2i\pi k/p}$ and similarly for k'. Then*

$$\xi(k) \bullet \xi(k') = C'_k \wedge C_k$$

where $C_{k'} \wedge C_k$ is the number of intersection of $C_{k'}$ by C_k (equal to $1, 0$ or -1 according to the trigonometric orientation of the unit circle).



Proof. See [Mer96] Lemma 4. □

3.4 Two useful formulas

Because of their technical aspect, we will not reproduce the proofs of the following formulas which appear in Lemmas 2 and 3 of [Mer96].

We have first a formula for $t_r e$ $(r > 1)$ in terms of the Manin symbols $\xi(k)$:

Proposition 2 (Merel). *Let $r < p$ be a positive integer. Then*

$$t_r e = - \sum_{\left(\begin{smallmatrix} u & v \\ w & t \end{smallmatrix}\right) \in X_r} \xi(w/t)$$

where X_r is the set of matrices $\left(\begin{smallmatrix} u & v \\ w & t \end{smallmatrix}\right)$ of determinant r such that $0 < w < t$ and $u > v \geq 0$.

For $r = 1$, we can compute directly the intersection of e with a Manin's generator:

Proposition 3 (Merel). *For any $k \in \{1, \dots, p-1\}$ we have*

$$(p-1)e \bullet \xi(k) = \frac{k_* - k}{p}(p-1) - 12S(k,p),$$

where $S(k,p) = \sum_{h=0}^{p-1} \bar{B}_1(\frac{h}{p})\bar{B}_1(\frac{kh}{p})$ is the Dedekind sum*, $\bar{B}_1$ the first Bernoulli polynomial made 1-periodic.*

Remark 3. Note that in Proposition 2 the $\xi(0)$ and $\xi(\infty)$ terms vanish. This is not surprising since $t_r e$ lies in the absolute homology group.

3.5 Conclusion of the proof

We will now explain substantially how Merel put all the previous ingredients together to obtain the proof of $(\star)$ for p great enough.

Suppose that there are integers $\lambda_1, \dots, \lambda_d$ such that

$$\lambda_1 e + \lambda_2 t_2 e + \cdots + \lambda_d t_d e = 0.$$

We will show successively that $\lambda_i = 0$ for all $i \in \{1, \dots, d\}$, treating the case of λ_1 independently.

Case $i = 1$. We look for x_1 of the form $x_1 = \xi(k)$ for some k such that

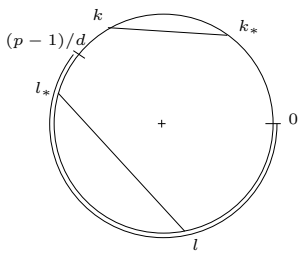
$$i)\ e \bullet \xi(k) \neq 0 \qquad \text{and} \qquad ii)\ t_r e \bullet \xi(k) = 0 \quad (1 < r \leq d)$$

Suppose that $p > d$. By Proposition 2, the condition $ii)$ is equivalent to

$$\sum_{\left(\begin{smallmatrix} u & v \\ w & t \end{smallmatrix}\right) \in X_r} \xi(w/t) \bullet \xi(k) = 0 \qquad (1 \leq r \leq d).$$

It suffices to find k such that $\xi(w/t) \bullet \xi(k) = 0$ for all $\left(\begin{smallmatrix} u & v \\ w & t \end{smallmatrix}\right) \in X_r$. That is what Merel does. Let $l \in \{1, \dots, p-1\}$ such that $l \equiv wt^{-1} \pmod p$ for some $\left(\begin{smallmatrix} u & v \\ w & t \end{smallmatrix}\right) \in X_r$. Then $l_* \equiv -tw^{-1} \pmod p$. By the Remark 3, we can suppose that neither t nor w are divisible by p.

Exercise 2. *Show that l and l_* are larger than $\frac{p-1}{d}$.*



Applying the *lemme des cordes* it suffices to find k such that both the complex numbers $e^{2i\pi k/p}$ and $e^{2i\pi k_*/p}$ are in a portion of the circle where $e^{2i\pi l/p}$ can not be, so for instance, by the exercise, such that both k and k_* lie in $[0, \frac{p-1}{d}[$. Merel uses then the following analytic lemma ([Mer96] Lemma 5) to ensure that, provided that $p > d^{3d^2}$, it suffices to choose some $k \in \mathbb{Z} \cap]\frac{p}{10d}, \frac{p}{5d} + 1[$ and then $k_* \in \mathbb{Z} \cap]\frac{p}{2d} - 1 - \frac{1}{d}, \frac{p-1}{d}[$ (more precisely, it is already true when $p/log^4(p) > d^4$).

Lemma 2. *Let p be a prime number and $a, b \geq 1$ two real numbers. Let $A, B \subset \{1, \dots, p-1\}$ be two intervals of cardinality p/a and p/b respectively. If $p > a^2 b^2 \log^4(p)$ then there exists $k \in A$ such that $k_* \in B$.*

We deduce from the following exercise that the condition $i)$ is also verified assuming that $p > d^{3d^2}$.

Exercise 3. *Using the Dedekind's reciprocity formula*

$$12(S(k,p)+S(p,k)) = -3 + \frac{p}{k} + \frac{k}{p} + \frac{1}{pk}$$

and the inequality $|12S(p,k)| \leq k$, *show that*

$$e \bullet \xi(k) \geq \frac{p}{10d} - 10d - 2$$

for all k *as before.*

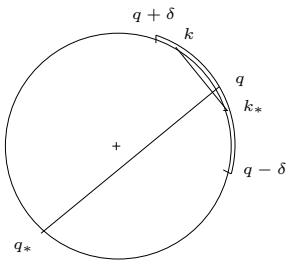
Case $i > 1$. Suppose now that

$$\lambda_2 t_2 e + \cdots + \lambda_c t_c e = 0$$

for some $c \leq d$. The method is almost the same as before: we look for $x_c = \xi(k)$ such that

$$i)\ t_c e \bullet \xi(k) \neq 0 \qquad \text{and} \qquad ii)\ t_r e \bullet \xi(k) = 0 \quad (2 \leq r < c).$$

We remark that in the formulas for $t_r e, r = 2 \ldots c$ of Proposition 2, the Manin symbol $\xi(1/c)$ occurs only in $t_c e$ and not in $t_r e$ for $r < c$. So we will look for k such that $\xi(1/c) \bullet \xi(k) = \pm 1$ and $\xi(w/t) \bullet \xi(k) = 0$ for all $\left(\begin{smallmatrix} u & v \\ w & t \end{smallmatrix}\right) \in X_r$ $(r \leq c)$ such that $w/t \neq 1/c$.



Let q and l in $\{1, \ldots, p-1\}$ such that $q \equiv 1/c \pmod p$ and $l \equiv w/t \neq 1/c \pmod p$ for some $\left(\begin{smallmatrix} u & v \\ w & t \end{smallmatrix}\right) \in X_r$ $(r \leq c)$.

Exercise 4. *Show that* $|l - q| \geq \delta$ *where* $\delta = \frac{p-d^2}{d(d-1)}$.

By the same analytic lemma as before, it is possible to find $k \in]q, q+\delta]$ such that $k_* \in [q-\delta, q[$ and $q_* \notin [q-\delta, q+\delta]$ when p is great enough, more precisely when $p/\log^4(p) > \mathrm{Sup}(d^8, 400d^4)$. By the lemme des cordes, it forces then λ_c to be zero.

This finishes the proof of Theorem 2.

3.6 Oesterlé's variant

As we said in Remark 1, Oesterlé improved the Merel's bound for the torsion of elliptic curves. For this, Oesterlé proved directly the formal immersion in positive characteristic:

Proposition 4. *Suppose that $p/\log^4 p \geq (2d)^6$. Then for all $l \geq 3$, the condition $(\star_l)$ is true, that is to say $\phi^{(d)}_{A,\mathbb{F}_l}$ is a formal immersion at $\infty^{(d)}_{\mathbb{F}_l}$.*

For $d \geq 33$, Theorem 2 with the bound $(3^{d/2}+1)^2$ then follows directly from Theorem 4, since $p > (3^{d/2}+1)^2$ implies $p/\log^4 p \geq (2d)^6$ in that case. Oesterlé studied the cases $d < 37$ by computations.

Let us give a sketch of proof of Proposition 4. Let T'_s defined by $T_r = \sum_{s|r} T'_s$ for all $r \geq 1$ and, instead of $t_r = T_r - \sigma'(r)$, $(r \geq 1)$, consider the following generators of the Eisenstein ideal I :

$$I_1 = n_p \quad \text{and} \quad I_r = \begin{cases} T'_r - r & \text{if } p \not| r \\ T'_r & \text{if } p|r \end{cases} (r \geq 2),$$

where we denote by n_p the numerator of $(p-1)/12$. We have $t_r = \sum_{s|r, s\neq 1} I_s$ for all $r > 1$.

Proposition 5. *If the images of $I_2e, \ldots, I_{2d}e$ in Ie/lIe are $\mathbb{F}_l$-linearly independent, then $T_1e, \ldots, T_de$ are $\mathbb{F}_l$-linearly independent in $\mathbb{T}e/l\mathbb{T}e$ that is to say $(\star_l)$ is true.*

Proof. We have

$$T'_2T'_r = \begin{cases} I_{2r} - 2I_r & \text{if } r \text{ is odd} \\ I_{2r} - 3I_r + 2I_{r/2} & \text{if } r \text{ is even.} \end{cases}$$

So if $I_2.e, \ldots, I_{2r}e$ are linearly independent in Ie/lIe, so do $T'_2e, \ldots, T'_2T'_{2r}e$ and, since $T'_2e = (T_2 - 3)e \in Ie$, we obtain that $T'_1e, \ldots, T'_de$ are linearly independent in $\mathbb{T}e/l\mathbb{T}e$. But $T_r = T'_r + \sum_{s|r, s<r} T'_s$ so $T_1e, \ldots, T_de$ are linearly independent in $\mathbb{T}e/l\mathbb{T}e$. □

Moreover, Oesterlé used Proposition 2 and the *lemme des cordes* to give an explicit formula for $t_re \bullet \xi(k)$ and then for $I_re \bullet \xi(k)$ (which is the unique "r-th term" of $t_re \bullet \xi(k)$) :

$$I_re \bullet \xi(k) = \left[\frac{rk}{p}\right] - \left[\frac{rk_*}{p}\right] + v_r(k) - v_r(k_*) \quad (r \geq 2, k \in \{1, \ldots, p-1\}), \quad (1)$$

where $v_r(k) = \sharp\{(a, a', b, b') \in \mathbb{Z}, a, a', b, b' \geq 1, aa' + bb' = r, (a, b) = 1, bk \equiv a \pmod p\}$. The end of the proof is then *mutatis mutandi* the same as Merel's one: using Lemma 2, Oesterlé showed that, when $p/log^4(p) > d^6$, it is possible for each $r \geq 2$ to find k such that $I_re \bullet \xi(k) = 1$ and $I_se \bullet \xi(k) = 0$ for $s < r$. He

deduced that for $p/log^4(p) > d^6$, $I_2e, \ldots, I_de$ are linearly independent. Applying this for $2d$ instead of d and using Proposition 5 gives Proposition 4.

This is how one can obtain Oesterlé's bound. As we said in Remark 2, the question of finding a bound growing polynomially in d remains open.

Remark 4. As Merel pointed out to me, the result of Proposition 5 is still true replacing I_r by t_r, $(2 \leq r \leq 2d)$. Indeed, a calculus proves that $t_2T_i \in t_{2i} + \sum_{1\leq j\leq i} \mathbb{Z}T_j$. Using the results of the section 3.5 case $i > 1$, it follows that when $p/\log^4(p) > \mathrm{Sup}(d^8, 400d^4)$, $(\star_l)$ is true for all $l \geq 3$. Since $p > (3^{d/2}+1)^2$ implies $p/\log^4(p) > \mathrm{Sup}(d^8, 400d^4)$ provided that $d \geq 37$, it gives the Oesterlé's bound in that case. The other cases have been studied by Oesterlé.

References

[Abr95] D. Abramovich. Formal finiteness and the torsion conjecture on elliptic curves. A footnote to a paper: "Rational torsion of prime order in elliptic curves over number fields" [Astérisque No. 228 (1995), 3, 81–100; MR1330929 (96c:11058)] by S. Kamienny and B. Mazur. *Astérisque*, (228):3, 5–17, 1995. Columbia University Number Theory Seminar (New York, 1992).

[Cas66] J. W. S. Cassels. Diophantine equations with special reference to elliptic curves. *J. London Math. Soc.*, 41:193–291, 1966.

[dar] *Summer school in arithmetic geometry.*

[Dem72] V. A. Dem′janenko. The boundedness of the torsion of elliptic curves. *Mat. Zametki*, 12:53–58, 1972.

[Edi95] B. Edixhoven. Rational torsion points on elliptic curves over number fields (after Kamienny and Mazur). *Astérisque*, (227):Exp. No. 782, 4, 209–227, 1995. Séminaire Bourbaki, Vol. 1993/94.

[Kam92] S. Kamienny. Torsion points on elliptic curves over fields of higher degree. *Internat. Math. Res. Notices*, (6):129–133, 1992.

[KM95] S. Kamienny and B. Mazur. Rational torsion of prime order in elliptic curves over number fields. *Astérisque*, (228):3, 81–100, 1995. With an appendix by A. Granville, Columbia University Number Theory Seminar (New York, 1992).

[Man72] Ju. I. Manin. Parabolic points and zeta functions of modular curves. *Izv. Akad. Nauk SSSR Ser. Mat.*, 36:19–66, 1972.

[Maz77] B. Mazur. Modular curves and the Eisenstein ideal. *Inst. Hautes Études Sci. Publ. Math.*, (47):33–186 (1978), 1977.

[Maz78] B. Mazur. Rational isogenies of prime degree (with an appendix by D. Goldfeld). *Invent. Math.*, 44(2):129–162, 1978.

[Mer96] L. Merel. Bornes pour la torsion des courbes elliptiques sur les corps de nombres. *Invent. Math.*, 124(1-3):437–449, 1996.

[Oes] J. Oesterlé. Torsion des courbes elliptiques sur les corps de nombres.

[Par99] P. Parent. Bornes effectives pour la torsion des courbes elliptiques sur les corps de nombres. *J. Reine Angew. Math.*, 506:85–116, 1999.