Local-Global principle for Torsion

Sebastiano Tronto

November 6, 2018

Introduction

We will follow the first pages of the paper *Galois Properties of Torsion Points on Abelian Varieties* by N. M. Katz. We will give the main result and prove that the problem reduces to a statement about representation theory, but we will not give the proof of the results themselves.

As an application, we compute the torsion points of some elliptic curves (not in these notes).

1 The Problem

Let A be an abelian variety over a number field K. Recall the following important Theorem:

Theorem 1.1 (Mordell-Weil)**.** *Let A be an abelian variety over a numebr field K. The group of K-rational points of A is a finitely generated abelian group.*

Proof. See [2], Theorem C.0.1 or [5], Chapter VIII for the case of elliptic curves. □

Corollary 1.2. *The torsion part $A(K)_{\text{tors}}$ of $A(K)$ is finite.*

The following fact is maybe less well-known, but it will be fundamental for us.

Lemma 1.3. *Let $\mathfrak{p}$ be a prime of K lying over the rational prime p and let $e_\mathfrak{p}$ be the absolute ramification of K at p (i.e. $p\mathcal{O}_K = \mathfrak{p}^{e_\mathfrak{p}}$). Assume that A has good reduction at $\mathfrak{p}$ and that $e_\mathfrak{p} < p - 1$. Then the reduction map $A(K) \to A(k_\mathfrak{p})$ is injective on the torsion points.*

Proof. See the appendix of [3]. □

Corollary 1.4. *For all but finitely many place of K we have $\#A(K)_{\text{tors}} \,|\, \#A(k_\mathfrak{p})$.*

Question: does the converse, in some sense, hold? For elliptic curves we have affirmative answer, but only *up to isogeny.*

2 Interlude - More Facts on Elliptic Curves

Let E be an elliptic curve over a field K and let ℓ be a rational prime with $\operatorname{char} K \neq \ell$. Fix an algebraic closure $\overline{K}$ of K.

For every $n \geq 1$ we have that $E[\ell^n] \cong (\mathbb{Z}/\ell^n\mathbb{Z})^2$ is a free $\mathbb{Z}/\ell^n\mathbb{Z}$-module of rank 2. Since any morphism of elliptic curves sends ℓ^n-torsion points to ℓ^n-torsion points, we have an action of the absolute Galois group of K on $E[\ell^n]$, i.e. we have a *Galois representation*

$$\overline{\rho}_{\ell^n} : \operatorname{Gal}\left(\overline{K} \,|\, K\right) \to \operatorname{Aut}_{\mathbb{Z}/\ell^n\mathbb{Z}}\left(E[\ell^n]\right) \cong \operatorname{GL}_2\left(\mathbb{Z}/\ell^n\mathbb{Z}\right) \tag{1}$$

where the isomorphism comes from choosing a $\mathbb{Z}/\ell^n\mathbb{Z}$-basis for $E[\ell^n]$.

If we want to consider all the ℓ-power torsion at once, we can take the projective limit with respect to transition maps $E[\ell^{n+1}] \to E[\ell^n]$ given by multiplication by ℓ. The $\mathbb{Z}_\ell$-module

$$T_\ell(E) := \varprojlim_n E[\ell^n] \cong \mathbb{Z}_\ell^2$$

is called the *Tate module* of E. Moreover, the representations as in (1) are compatible and they give rise to a representation

$$\rho_\ell : \mathrm{Gal}\left(\overline{K} \,|\, K\right) \to \mathrm{Aut}_{\mathbb{Z}_\ell} T_\ell(E) \cong \mathrm{GL}_2(\mathbb{Z}_\ell)$$

such that the diagrams of the form

$$\begin{array}{ccc} \mathrm{Gal}\left(\overline{K} \,|\, K\right) & \xrightarrow{\rho_\ell} & \mathrm{GL}_2(\mathbb{Z}_\ell) \\ & \searrow^{\overline{\rho}_{\ell^n}} & \downarrow \\ & & \mathrm{GL}_2(\mathbb{Z}/\ell^n\mathbb{Z}) \end{array}$$

commute.

Moreover, we define

$$K(E[\ell^n]) := \overline{K}^{\ker \overline{\rho}_{\ell^n}}$$

which is a finite extension of K, given by adjoining the coordinates of all torsion points of E. By definition we have $\mathrm{Gal}(K(E[\ell^n]) \,|\, K) \cong \mathrm{Im}\, \overline{\rho}_{\ell^n}$.

Proposition 2.1. *Let $\phi : E \to E$ be an endomorphism and let ϕ_ℓ be the induced map on $T_\ell(E)$. Then $\det(\phi_\ell)$ and $\mathrm{tr}(\phi_\ell)$ are independent of the prime ℓ.*

Proof. See [5], Proposition III.8.6. □

In view of the proposition above, for any endomorphism $\phi : E \to E$ we can define $\det \phi := \det(\phi_\ell)$ and $\mathrm{tr}\, \phi := \mathrm{tr}(\phi_\ell)$. It makes also sense to define the characteristic polynomial f_ϕ^{char} of ϕ to be the characteristic polynomial of any ϕ_ℓ.

Proposition 2.2. *Let E be an elliptic curve over a finite k and let $F \in \mathrm{Gal}(\overline{k} \,|\, k)$ be the Frobenius. Then the characteristic polynomial of F is*

$$f_{F_\mathfrak{p}}^{\mathrm{char}}(T) = T^2 - aT + \#k$$

where $a = 1 + \#k - \#E(k)$. In particular, we have $\#E(k) = \det(1 - F)$.

Proof. See [5], Theorem V.2.3.1. □

With this we can prove the following result.

Lemma 2.3. *Let E_1, E_2 be two elliptic curves over a finite field k. If E_1 and E_2 are k-isogenous, we have $\#E_1(k) = \#E_2(k)$.*

Proof. Let $\phi : E_1 \to E_2$ be an isogeny defined over k and let F be the Frobenius of k. We claim that the characteristic polynomial f_1 for F as endomorphism of E_1 is the same as that of F as an endomorphism of E_2, which is enough to conclude.

To prove the claim, let $P \in E$ be any point. Then $O_{E_2} = \phi(O_{E_1}) = \phi(f_1(F)(P)) = f_1(F)(\phi(P))$ because ϕ, being defined over k, commutes with $f_1(F)$. Since P was arbitrary and ϕ is surjective, we have $f_1(F)(Q) = O_{E_2}$ for all $Q \in E_2$, thus $f_1(F) = 0$ as an endomorphism of E_2. This means that f_1 si the characteristic polynomial of F as an endomorphism of E_2. □

Remark 2.4. The converse is also true, as a consequence of Tate's Isogeny Theorem.

3 Main Results and Some Consequences

The main result of [3] is the following.

Theorem 3.1. *Let A be an elliptic curve over a number field K. Let m be a positive integer such that $m \mid \#A(k_\mathfrak{p})$ for all but finitely many primes $\mathfrak{p}$. There exists an elliptic curve A' that is K-isogenous to A and such that $m \mid \#A'(K)_{\text{tors}}$.*

Remark 3.2. In Theorem 3.1 it is enough to assume that $m \mid \#A(k_\mathfrak{p})$ holds for a set of primes of Dirichlet density 1.

Theorem 3.1 is equivalent to the following.

Theorem 3.3. *Let A be an elliptic curve over a number field K. Let ℓ be a prime and $n \geq 1$ an integer. Assume that $\ell^n \mid \#A(k_\mathfrak{p})$ for all but finitely many primes $\mathfrak{p}$. There exists an elliptic curve A' that is K-isogenous to A via an ℓ-power-degree isogeny such that $\ell^n \mid \#A'(K)_{\text{tors}}$.*

Proof of equivalence. Assume that Theorem 3.1 holds. We know that such A' exists, together with a K-isogeny $\varphi : A \to A'$ of not necessarily ℓ-power degree. Let $M = \ker \varphi$ and let M_ℓ be the ℓ-primary part of M. Then $\pi : A \to A/M_\ell$ of ℓ-power degree and φ factors via π as an isogeny $\psi : A/M_\ell \to A'$ of degree prime to ℓ. Thus ψ is an isomorphism on the ℓ^∞-torsion points, and we conclude by replacing A' with A/M_ℓ.

For the converse, we procede by induction on the number of prime factos of m. The base case (i.e., m is a prime power) is given directly by Theorem 3.3. Assume now that $m = m_1 \ell^n$ with $\ell \nmid m_1$. Let $\psi : A \to A'$ be an isogeny, which we can assume of degree not divisible by ℓ, with A' such that $m_1 \mid \#A'(K)_{\text{tors}}$. By Lemma 2.3 we have $\ell^n \mid \#A'(K)_{\text{tors}}$, so there exists an isogeny $\varphi : A' \to A''$ of ℓ-power degree such that $\ell^n \mid \#A''(K)_{\text{tors}}$. Moreover, φ is an isomorphism on the m_1-torsion part, so we conclude by taking the isogeny $\varphi \circ \psi$. □

Remark 3.4. The case $n = 1$ of Theorem 3.3 holds for abelian surfaces as well, while Theorem 3.1 fails in this case. In dimension 3 or higher everything fails.

Moreover, since $\ell \mid \#A(k_\mathfrak{p}) \iff A(k_\mathfrak{p})$ has ℓ-torsion, the $n = 1$ case of Theorem 3.1 can be rephrased as an (almost everywhere) *local-global principle*: the existence of ℓ-torsion points at almost all the reductions implies the existence of global ℓ-torsion points.

We can see that the results above imply the following proposition. In some sense, it tells us that there exists an elliptic curve K-isogenous to A that has "all the possible rational torsion".

Proposition 3.5. *Let A be an elliptic curve over a number field K. There exists a positive integer N that divides $\#A(k_\mathfrak{p})$ for almost all $\mathfrak{p}$ and that is maximal with respect to this property. Moreover, there exists an elliptic curve A_N which is K-isogenous to A and such that $\#A(K)_{\text{tors}} = N$.*

Proof. For any $n \geq 2$ let

$$a_n := \gcd\{A(k_\mathfrak{p}) \mid n \leq \#k_\mathfrak{p}\} = \lim_{m \to +\infty} \gcd\{A(k_\mathfrak{p}) \mid n \leq \#k_\mathfrak{p} \leq m\}$$

and define $V_\ell := \lim_{n \to +\infty} v_\ell(a_n)$ for all primes ℓ.

We claim that $V_\ell < \infty$ for all primes ℓ. It is in fact a deep result (due to Faltings, see [1]) that, up to isomorphism, there are only finitely many elliptic curves isogenous to A via an ℓ-power-degree isogeny. Since for any $n \leq$ we have that $\ell^n \mid \#A(k_\mathfrak{p})$ for almost all $\mathfrak{p}$, the claim follows from Theorem 3.3.

Moreover we have $V_\ell = 1$ for all but finitely many ℓ, again by Theorem 3.3 and using the fact that the kernel of an isogeny of degree ℓ^d is a subgroup of $A(K)_{\text{tors}}$ with ℓ^d elements. In fact, by a Theorem of Merel [4], if any elliptic curve over K has a point of order ℓ than $\ell < [K : \mathbb{Q}]^{3[K:\mathbb{Q}]^2}$. If $\ell \neq 1$ some ℓ greater than this bound, then Theorem 3.3 would be in contradiction with this result.

Let then $N = \prod_\ell V_\ell$. Clearly N is the biggest integer dividing $\#A(k_\mathfrak{p})$ for almost all $\mathfrak{p}$. The last part follows directly from Theorem 3.1. □

4 Reduction to Representation Theory

Theorem 4.1 (Чеботарёв's Density Theorem)**.** *Let $L \mid K$ be a finite Galois extension with Galois group G. Let $X \subseteq G$ be a union of conjugacy classes. Then the set of primes $\mathfrak{p}$ of K that are unramified in L and such that the Frobenius at $\mathfrak{p}$ is in X has density $\#X/\#G$.*

Corollary 4.2. *Let A be an elliptic curve over a number field K and let ℓ be a rational prime. Then*

$$\det(1-g) \equiv 0 \pmod{\ell^n} \qquad \text{for all } g \in \mathrm{Gal}(\overline{K} \mid K)$$

if and only if

$$\ell^n \mid \#A(k_\mathfrak{p}) \qquad \text{for almost all primes } \mathfrak{p} \text{ of } K.$$

Proof. Let $\mathfrak{p}$ be a prime of good reduction for A. Since $\det(1-F_\mathfrak{p}) = \#A(k_\mathfrak{p})$, the "only if" part is trivial.

For the "if" part, we use Чеботарёв's Density Theorem. Let $L = K(A[\ell^n])$ and

$$X = \{g \in \mathrm{Gal}(L \mid K) \mid \det(1 - \overline{\rho}_{\ell^n}(g)) = 0\}.$$

Then for almost all $\mathfrak{p}$ we have $F_\mathfrak{p} \in X$, so it must be $X = \mathrm{Gal}(L \mid K)$. By commutativity of the diagram

$$\begin{array}{ccccc} \mathrm{Gal}(\overline{K} \mid K) & \xrightarrow{\rho_\ell} & \mathrm{GL}_2(\mathbb{Z}_\ell) & \xrightarrow{\det} & \mathbb{Z}_l \\ \downarrow & & \downarrow & & \downarrow \\ \mathrm{Gal}(L \mid K) & \xrightarrow{\overline{\rho}_{\ell^n}} & \mathrm{GL}_2(\mathbb{Z}/\ell^n\mathbb{Z}) & \xrightarrow{\det} & \mathbb{Z}/\ell^n\mathbb{Z} \end{array}$$

we conclude. □

Corollary 4.3. *The integer N of Proposition 3.5 divides $\#E(k_\mathfrak{p})$ for all $\mathfrak{p}$ of good reduction for E.*

Thanks to the Corollary we can rephrase Theorem 3.3 as follows.

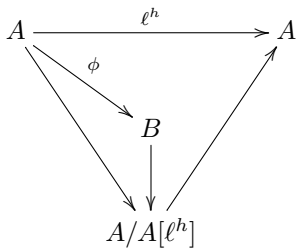
Theorem 4.4. *Let A be an elliptic curve over a number field K. Let ℓ be a prime and $n \geq 1$ an integer. Assume that $\det(1-g) \equiv 0 \pmod{\ell^n}$ for all $\gamma \in \mathrm{Gal}(\overline{K} \mid K)$. There exists an elliptic curve A' that is K-isogenous to A via an ℓ-power-degree isogeny such that $\ell^n \mid \#A'(K)_{\mathrm{tors}}$.*

We also need the following general fact.

Proposition 4.5. *Let A be an elliptic curve over a number field K and let ℓ be a rational prime. There is a one-to-one correspondence between isomorphism classes of elliptic curves A' over K that are K-isogenous to A via an isogeny of ℓ-power degree and $\mathrm{Gal}(\overline{K} \mid K)$-stable lattices in $V_\ell = T_\ell(A) \otimes \mathbb{Q}$.*

Sketch of proof. If $\phi : A \to B$ is an isogeny, then $\phi : T_\ell(A) \to T_\ell(B)$ is injective and $\phi_\ell : V_\ell(A) \to V_\ell(B)$ is an isomorphism. Thus it sends $T_\ell(A)$ to some other lattice in $V_\ell(A)$. Since ϕ is defined over K, this lattice is Galois-stable.

Conversely, let $\Lambda \subseteq V_\ell(A)$ be any Galois-stable lattice. Let $k, h \geq 1$ be integers such that $\ell^h T_\ell(A) \subseteq \ell^k \Lambda \subseteq T_\ell(A)$ and let $N = \mathrm{Im}(\ell^k \to T_\ell(A)/\ell^h T_\ell(A)) \subseteq A[\ell^h]$, which is a finite subgroup of A. Let $B := A/N$ and let $\varphi : A \to B$ be the quotient map. We have the following commutative diagram:



so there exists an isogeny $\psi : B \to A$ sich that $\psi \circ \phi = \ell^h$. Passing on the Tate modules we get $\psi_\ell(T_\ell(B)) \supseteq \ell^h T_\ell(A)$, so it is enough to show that $\psi_\ell(T_\ell(B))/\ell^h T_\ell(A) = N$. For any n we have

$$B[\ell^n] = \{a + N \mid a \in A,\, \ell^n a \in N\}$$

and since $\psi(a+N) = \ell^h a$ we get

$$\frac{\psi(T_\ell(B))}{\ell^h T_\ell(A)} = \frac{\{(\psi_\ell(a_k+N)_{k\in\mathbb{N}} = (\ell^k a_k)_{k\in\mathbb{N}} \,|\, a_k \in A,\, \ell^k a_k \in N,\, \ell a_{k+1} - a_k \in N \,\forall\, k\}}{\ell^h T_\ell(A)} =$$
$$= \{\ell^h a_h \,|\, a_h \in A,\, \ell^h a_h \in N\} =$$
$$= N.$$

So B is isogenous to A and such that $T_\ell(B) = \ell^k \Lambda$. Moreover, the fact that Λ is Galois-stable implies that the isogeny that we constructed is defined over K. Up to composing with multiplication by ℓ^k, we may assume that $T_\ell(B) = \Lambda$. □

With this fact we get the equivalent formulation that follows.

Theorem 4.6. *Let A be an elliptic curve over a number field K. Let ℓ be a prime and $n \geq 1$ an integer. Assume that $\det(1 - \rho_\ell(g)) \equiv 0 \pmod{\ell^n}$ for all $\gamma \in \mathrm{Gal}(\overline{K} \,|\, K)$. There exist $\mathrm{Gal}(\overline{K} \,|\, K)$-stable lattices $\Lambda \supseteq \Lambda'$ in $V_\ell(A)$ such that $\#(\Lambda/\Lambda') = \ell^n$ and $\mathrm{Gal}(\overline{K} \,|\, K)$ acts trivially on Λ/Λ'.*

Proof of equivalence with Theorem 4.4. If Theorem 4.4 holds, we can let Λ be the lattice corresponding to A' and Λ' that corresponding to A'/N, where $N \subseteq A'(K)$ is any group of rational torsion points of order ℓ^n. Vice-versa, we can let A' be the elliptic curve corresponding to Λ; the existence of an elliptic curve B corresponding to Λ' and of a K-isogeny $\phi : A' \to B$ assures that $\ker \phi \subseteq A'(K)$ is a group of rational torsion points of order ℓ^n. □

Our theorem is then a consequence of the following result, which is purely about representation theory.

Proposition 4.7. *Let ℓ be a prime number, $n \geq 1$ an integer, V a two-dimensional $\mathbb{Q}_\ell$-vector space and $G \subseteq \mathrm{Aut}_{\mathbb{Q}_\ell}(V)$ a compact subgroup. If $\det(1-g) \equiv 0 \pmod{\ell^n}$ for every $g \in G$, then there exist G-stable lattices $\Lambda \supseteq \Lambda'$ such that $\#(\Lambda/\Lambda') = \ell^n$ and such that the action of G on Λ/Λ' is trivial.*

References

[1] G. Cornell, J. H. Silverman, *Arithmetic Geometry*, 1986.

[2] M. Hindry, J. H. Silverman, *Diophantine Geometry*, 2000.

[3] N. M. Katz, *Galois Properties of Torsion Points on Abelian Varieties*, 1981.

[4] L. Merel, *Bornes pour la torsion des courbes elliptiques sur les corps de nombres*, 1996.

[5] J. H. Silverman, *The Arithmetic of Elliptic Curves*, Second Edition (2016).