Galois representations on torsion points of elliptic curves
NATO ASI 2014 – Arithmetic of Hyperelliptic Curves and Cryptography

Francesco Pappalardi

Ohrid, August 25 - September 5, 2014

1 Lecture 1 - Introduction

Let $E/\mathbb{Q}$ be an elliptic curve. It is well known since the time of Jacobi that, for any field extension $K/\mathbb{Q}$, the set $E(K)$ of projective K–rational points has a natural group structure. Furthermore, if $K/\mathbb{Q}$ is finite, $E(K)$, with respect to this group structure, is finitely generated.

For any integer n, we consider the kernel of the *multiplication-by-n map*,

$$E[n] = \{P \in E(\overline{\mathbb{Q}}) : nP = \infty\}$$

which is called the *n–torsion subgroup*. It is part of the classical theory the fact that if n is an odd integer and $P(x, y, 1) \in E(\overline{\mathbb{Q}})$ is non zero, then $P \in E[n]$ if and only if x is a root of the *n–division polynomial* $\psi_n(X) \in \mathbb{Z}[X]$ which are defined by recursive formulas and are separable. Furthermore

$$\deg \psi_n = \frac{n^2 - 1}{2}.$$

This implies easily that if n is odd, then

$$E[n] \cong \mathbb{Z}/n\mathbb{Z} \times \mathbb{Z}/n\mathbb{Z}. \tag{1}$$

A similar argument allows to conclude that (1) holds also for n even. We set

$$E[\infty] = \bigcup_{n \in \mathbb{N}} E[n]$$

which is the *torsion subgroup* of $E(\overline{\mathbb{Q}})$. In virtue of (1), we have that

$$\mathrm{Aut}(E[n]) \cong \mathrm{GL}_2(\mathbb{Z}/n\mathbb{Z}).$$

So, there is a profinite group structure

$$\mathrm{Aut}(E[\infty]) \cong \mathrm{GL}_2(\hat{\mathbb{Z}}) \quad \text{where} \quad \hat{\mathbb{Z}} = \varprojlim \mathbb{Z}/n\mathbb{Z}.$$

The absolute Galois group

$$G_{\mathbb{Q}} := \mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q}) = \{\sigma : \overline{\mathbb{Q}} \to \overline{\mathbb{Q}}, \text{ field automorphism}\}$$

is also a profinite group and if K is any Galois extension of $\mathbb{Q}$, then

$$\mathrm{Gal}(K/\mathbb{Q}) \cong G_{\mathbb{Q}}/\{\sigma \in G_{\mathbb{Q}} : \sigma_{|_K} = \mathrm{id}_K\}.$$

So $G_{\mathbb{Q}}$ admits as quotient any possible Galois Group of Galois extensions of $\mathbb{Q}$ and it is the projective limit of its finite quotients.

For every integer n, we consider the *n–torsion field* $\mathbb{Q}(E[n])$ obtained by adjoining to $\mathbb{Q}$ all coordinates of all non zero points in $E[n]$. Finally we use $G(n)$ to denote the Galois group $\mathrm{Gal}(\mathbb{Q}(E[n])/\mathbb{Q})$.

If $P = (x, y, 1) \in E[n]$ and $\sigma \in G(n)$, then $\sigma P := (\sigma x, \sigma y, 1) \in E[n]$. This property and the fact that the operation in $E(\overline{\mathbb{Q}})$ is defined by $\mathbb{Q}$–rational functions, provides us with an inclusion

$$\rho_n : G(n) \hookrightarrow \mathrm{Aut}(E[n]) \cong \mathrm{GL}_2(\mathbb{Z}/n\mathbb{Z})$$

which can be extended to

$$\rho : G_{\mathbb{Q}} \longrightarrow \mathrm{Aut}(E[\infty]) = \prod_{\ell \text{ prime}} \mathrm{Aut}(E[\ell^\infty]) \cong \prod_{\ell \text{ prime}} \mathrm{GL}_2(\mathbb{Z}_\ell).$$

where $E[\ell^\infty] = \cup_{m \in \mathbb{N}} E[\ell^m]$ and $\mathbb{Z}_\ell$ denoted the ring of *ℓ–adic integers*. The above representation is an object of study during these three lectures.

The main result of the Theory is

Theorem (Serre's Uniformity Theorem)**.** *If E does not have complex multiplication (i.e. the only homomorphism $E(\overline{\mathbb{Q}}) \to E(\overline{\mathbb{Q}})$ which are defined by rational maps are the* multiplication-by-n maps*), then the index of $\rho_n(G(n))$ inside* $\mathrm{Aut}(E[n])$ *is bounded by a constant that depends only on E.*

This statement has several striking consequences among which:

Corollary. *If E does not have complex multiplication, then for all ℓ large enough*

$$G(\ell) = \mathrm{Aut}(E[\ell])$$

One of the central problem of this theory is to establish explicit bounds for ℓ for which the conclusion of the above Corollary holds. It is believed that it holds for all $\ell > 37$.

The group homomorphism

$$\rho_{\ell^\infty} : G_{\mathbb{Q}} \to \mathrm{Aut}(E[\ell^\infty])$$

obtained by composing ρ with the projection on the ℓ-th component, is actually a continuous homomorphism of topological groups and it is called *ℓ–adic representation.*

The representation ρ_{ℓ^∞} is *unramified* at all primes $p \nmid \ell\Delta_E$ in the sense that for such primes $\rho_\ell|_{I_\mathfrak{p}} = \mathrm{Id}_{\mathbb{Z}_\ell}$ where, for a fixed prime number p and a fixed prime $\mathfrak{p}$ of $\bar{\mathbb{Q}}$ over p, one defines the *inertia subgroup* $I_\mathfrak{p} \subset G_{\mathbb{Q}}$ as the set of those elements of $G_{\mathbb{Q}}$ such that

$$\sigma(x) \equiv x \bmod \mathfrak{p}, \quad \forall x \in \bar{\mathbb{Z}}.$$

Serre's Uniformity Theorem is equivalent to the conjunction of the following two statements:

- For all primes ℓ, $\rho_{\ell^\infty}(G_{\mathbb{Q}})$ is an open subgroup with respect to the ℓ–adic topology,
- For all but finitely many primes ℓ, $\rho_{\ell^\infty}(G_{\mathbb{Q}}) = \mathrm{Aut}(E[\ell^\infty])$.

An important tool in the study of the above representations is the *Frobenius element*. In general, in a Galois extension K of $\mathbb{Q}$, for an unramified prime p, one defines the Frobenius element as any element in the conjugation class of the Galois Group $\mathrm{Gal}(K/\mathbb{Q})$ which is determined by the lift of the Frobenius automorphism of the finite field $\mathcal{O}_K/\mathcal{P}$ obtained as a quotient of the ring of integers $\mathcal{O}$ by any prime ideal $\mathcal{P}$ over p. Sometimes one calls *Artin symbol*, the conjugation class itself and denotes it by $\left[\frac{K/\mathbb{Q}}{p}\right]$.

In the case of the division fields $\mathbb{Q}(E[n])$, the Artin symbol can be thought as a conjugation class of matrices in $\mathrm{GL}_2(\mathbb{Z}/n\mathbb{Z})$. The characteristic polynomial $\det(\left[\frac{\mathbb{Q}(E[n])/\mathbb{Q}}{p}\right] - T)$ turns out not to depend on n in the sense that

$$\det\left(\left[\frac{\mathbb{Q}(E[n])/\mathbb{Q}}{p}\right]\right) \equiv p \bmod n, \qquad \mathrm{tr}\left(\left[\frac{\mathbb{Q}(E[n])/\mathbb{Q}}{p}\right]\right) \equiv a_E \bmod n$$

where $a_E = p - 1 - \#E(\mathbb{F}_p)$.

During the first lecture we will introduce the above notions and explain some of their properties.

2 Lecture 2 - Serre's Open Mapping Theorem and its applications

In most of Lecture 2 we will assume that E has no complex multiplication. During this lecture we will introduce more tools and notions necessary for later applications.

2.1 Chebotarev Density Theorem

If $K/\mathbb{Q}$ is a finite Galois extension and $\mathcal{C} \subset \mathrm{Gal}(K/\mathbb{Q})$ is a union if conjugation classes of $\mathcal{G} = \mathrm{Gal}(K/\mathbb{Q})$, then the *Chebotarev Density Theorem* predicts that the density of the primes p such that the Artin symbol $\left[\frac{K/\mathbb{Q}}{p}\right] \subset \mathcal{C}$ equals $\frac{\#\mathcal{C}}{\#\mathcal{G}}$. The Chebotarev Density Theorem has also a quantitative versions. Let

$$\pi_{\mathcal{C}/\mathcal{G}}(x) := \#\left\{p \le x : \left[\frac{K/\mathbb{Q}}{p}\right] \subset \mathcal{C}\right\}.$$

Then (see Serre [10] and Murty, Murty & Saradha [7]), assuming that the Dedekind zeta function of K satisfies the *Generalized Riemann Hypothesis*,

$$\pi_{\mathcal{C}/\mathcal{G}}(x) = \frac{\#\mathcal{C}}{\#\mathcal{G}} \int_2^x \frac{dt}{\log x} + O\left(\sqrt{\#\mathcal{C}}\sqrt{x}\log(xM\#\mathcal{G})\right)$$

where M is the product of primes numbers that ramify in $K/\mathbb{Q}$. An analogue version, independent on the Generalized Riemann Hypothesis can be found in [10].

We will apply it in the special case when $K = \mathbb{Q}(E[n])$ where we think at the element of $\mathcal{G}$ as 2 by 2 non singular matrices. For example

- In the case when $\mathcal{C} = \{\mathrm{id}\}$, the condition $\left[\frac{\mathbb{Q}(E[n])/\mathbb{Q}}{p}\right] = \{\mathrm{id}\}$ is equivalent to the property that

$$E[n] \subset \bar{E}(\mathbb{F}_p)$$

where $\overline{E}(\mathbb{F}_p)$ is the group of $\mathbb{F}_p$-rational points on the reduced curve $\overline{E}$.

- In the case when $\mathcal{C} = \mathcal{G}_{\mathrm{tr}=r} = \{\sigma \in \mathcal{G} : \operatorname{tr}\sigma = t\}$, and ℓ is a sufficiently large prime so that $\mathrm{Gal}(\mathbb{Q}(E[\ell])/\mathbb{Q}) = \mathrm{GL}_2(\mathbb{F}_\ell)$, then

$$\#\,\mathrm{GL}_2(\mathbb{F}_\ell)_{\mathrm{tr}=r} = \begin{cases} \ell^2(\ell-1) & \text{if } r = 0 \\ \ell(\ell^2-\ell-1) & \text{otherwise.} \end{cases}$$

These examples will be elaborated during Lecture 3.

2.2 Classification of possible subgroups of $\mathrm{GL}_2(\mathbb{F}_\ell)$ that can appear as image of Galois

Part of the work of Serre consists in classifying the possible images of $G(\ell)$. More precisely, Serre proved in [9] that $\rho_\ell(G_\mathbb{Q})$ contains a subgroup of one of the following types:

1. "split half Cartan subgroup": A cyclic subgroup of of $\ell - 1$ which can be represented as

$$\left\{\begin{pmatrix} a & 0 \\ 0 & 1 \end{pmatrix} : a \in \mathbb{F}_\ell^*\right\},$$

2. "half Borel subgroup": A solvable group that can be represented as

$$\left\{\begin{pmatrix} a & 0 \\ 0 & b \end{pmatrix} : a \in \mathbb{F}_\ell^*, b \in \mathbb{F}_\ell\right\},$$

3. "non split half Cartan subgroup": A cyclic subgroup of of $\ell^2 - 1$.

Furthermore if $\rho_\ell(G_\mathbb{Q}) \neq \mathrm{GL}_2(\mathbb{F}_\ell)$, then one of the following happens:

- $\rho_\ell(G_\mathbb{Q})$ is either contained in a Cartan subgroup or a Borel subgroup (upper triangular matrices) of $\mathrm{GL}_2(\mathbb{F}_\ell)$,
- $\rho_\ell(G_\mathbb{Q})$ is contained in the normalizer of a Cartan subgroup and it is not contained in the Cartan subgroup of $\mathrm{GL}_2(\mathbb{F}_\ell)$.

We will conclude with some explicit examples.

2.3 The Definition of Serre's Curve

It is in general not easy to compute the image $\rho(G_\mathbb{Q}) \subset \mathrm{GL}_2(\hat{\mathbb{Z}})$. Actually, it was showed by Serre that $\rho(G_\mathbb{Q})$ is always contained in an index 2 subgroup of $\mathrm{GL}_2(\hat{\mathbb{Z}})$. Such subgroup is called the *Serre's Subgroup* $\mathcal{H}_E$ and it is defined as

$$\mathcal{H}_E = \pi_{m_E}^{-1}(H_{m_E})$$

where

- $\pi_m : \mathrm{GL}_2(\hat{\mathbb{Z}}) \to \mathrm{GL}_2(\mathbb{Z}/m\mathbb{Z})$ is the natural projection,
- m_E is the *Serre number of* E defined as the least common multiple $[2, \mathrm{disc}(\mathbb{Q}(\sqrt{|\Delta_E|}))]$,
- and if ε denotes the *signature map* (i.e. $\varepsilon : \mathrm{GL}_2(\mathbb{Z}/m\mathbb{Z}) \to \mathrm{GL}_2(\mathbb{Z}/2\mathbb{Z}) \cong S_3 \to \{\pm 1\}$), then

$$H_m = \left\{\sigma \in \mathrm{GL}_2(\mathbb{Z}/m\mathbb{Z}) : \varepsilon(A) = \left(\frac{\Delta_E}{\det A}\right)\right\}.$$

An elliptic curve $E/\mathbb{Q}$ is called *a Serre curve* if $\rho(G_\mathbb{Q}) = \mathcal{H}_E$. These curves are quite common and will be considered in the third lecture.

3 Lecture 3 - The Lang–Trotter Conjectures

The third lecture is devoted to reviews of some applications of ℓ–adic representations to number Theory and in particular to the Lang–Trotter Conjectures.

3.1 Lang Trotter for primitive points

E. Artin made a celebrated conjecture concerning the density of primes for which a given integer is a primitive root. In the first part of this lecture, we will discuss an analogous conjecture for elliptic curves. Let E be an elliptic curve defined over $\mathbb{Q}$ with $P \in E(\mathbb{Q})$ a $\mathbb{Q}$-rational point of infinite order. P is called *primitive* for a prime p if the reduction $\overline{P}$ of P mod p generates the entire group $\overline{E}(\mathbb{F}_p)$ of $\mathbb{F}_p$-rational points on the reduced curve $\overline{E}$.

We set

$$\pi_{E,P}(x) = \#\{p \leq x : p \nmid \Delta_E \text{ and } P \text{ is primitive for } p\}.$$

In 1976, Lang and Trotter in [5] conjecture an asymptotic formula for $\pi_{E,P}(x)$ and consequently an expression for the density of primes for which P is primitive. More precisely, they conjecture that

$$\pi_{E,P}(x) \sim \delta_{E,P} \frac{x}{\log x} \qquad x \to \infty.$$

where

$$\delta_{E,P} = \sum_{n=1}^{\infty} \mu(n) \frac{\#\mathcal{C}_{P,n}}{\#\operatorname{Gal}(\mathbb{Q}(E[n], n^{-1}P)/\mathbb{Q})}$$

where $\mathbb{Q}(E[n], n^{-1}P)$ is the extension of $\mathbb{Q}(E[n])$ obtained with all the coordinates of the points $Q \in E(\bar{\mathbb{Q}})$ such that $nQ = P$ and $\mathcal{C}_{P,n}$ are suitable defined union of conjugacy classes in $\operatorname{Gal}(\mathbb{Q}(E[n], n^{-1}P)/\mathbb{Q})$.

The heuristic argument is based on the Chebotarev Density Theorem. The Lang–Trotter conjecture for primite points is still not known in any case. The Generalized Riemann Hypothesis allows to deduce some analogue conjectures for CM elliptic curves. We will discuss some of the known results and in particular those due to Gupta, Murty and Murty [3]

3.2 Serre's Cyclicity Conjecture

J. P. Serre has formulated a conjecture with a similar flavor. Let $E/\mathbb{Q}$ be an elliptic curve and let

$$\pi_E^{\text{cyclic}}(x) = \#\{p \leq x : \overline{E}(\mathbb{F}_p) \text{ is cyclic}\}.$$

The conjecture postulates the validity of the asymptotic formula:

$$\pi_E^{\text{cyclic}}(x) \sim \delta_E^{\text{cyclic}} \frac{x}{\log x} \qquad x \to \infty$$

where

$$\delta_E^{\text{cyclic}} = \sum_{n=1}^{\infty} \frac{\mu(n)}{\operatorname{Gal}(\mathbb{Q}(E[n])/\mathbb{Q})}.$$

Serre himself applied the Chebotarev Density Theorem, in analogy with the Hooley's work for Artin's Conjecture, and proved this conjecture as a consequence of the Generalized Riemann Hypothesis. Furthermore, if E has no CM, δ_E^{cyclic} is a rational multiple of the quantity

$$\prod_{\ell} \left(1 - \frac{1}{(\ell^2 - \ell)(\ell^2 - 1)}\right).$$

We will discuss this result and several more due to Gupta and Murty [4] and to A. Cojocaru [1].

3.3 Lang Trotter for fixed trace of Frobenius

In an earlier publication [6], Lang and Trotter considered, for a fixed elliptic curve $E/\mathbb{Q}$ and an integer r, the function

$$\pi_E^r(x) = \#\{p \leq x : p \nmid \Delta_E \text{ and } \#\overline{E}(\mathbb{F}_p) = p + 1 - r\}$$

and they conjecture that if either $r \neq 0$ or if E has no CM, then

$$\pi_E^r(x) \sim C_{E,r} \frac{\sqrt{x}}{\log x} \qquad x \to \infty$$

where $C_{E,r}$ is the so–called *Lang–Trotter constant* which is defined as follows:

$$C_{E,r} = \frac{2}{\pi} \lim_{m \to \infty} \frac{K_m \# \operatorname{Gal} \mathbb{Q}(E[K_m])/\mathbb{Q})_{\text{trace}=r}}{\# \operatorname{Gal} \mathbb{Q}(E[K_m])/\mathbb{Q})}$$

where K_m a sequence of integers with the property that every integer divides K_m when m is large enough. For example $k_m = m!$ has this property.

In virtue of the Open Mapping Theorem, we know that there exists an integer N_E, called the *torsion conductor* such that

$$C_{E,r} = \frac{2}{\pi} \frac{N_E \# \operatorname{Gal} \mathbb{Q}(E[N_E])/\mathbb{Q})_{\mathrm{trace}=r}}{\# \operatorname{Gal} \mathbb{Q}(E[N_E])/\mathbb{Q})} \times \prod_{\ell \nmid N_E} \frac{\ell \# \operatorname{GL}_2(\mathbb{F}_\ell)_{\mathrm{tr}=r}}{\# \operatorname{GL}_2(\mathbb{F}_\ell)}$$

As an application of the theory of ℓ–adic representations and of the Chebotarev density Theorem, assuming the Generalized Riemann Hypoythesis, Serre in [10] showed that

$$\pi_E^r(x) \ll \begin{cases} x^{7/8}(\log x)^{-1/2} & \text{if } r \neq 0 \\ x^{3/4} & \text{if } r = 0. \end{cases}$$

These results were improved for $r \neq 0$ by Murty, Murty and Sharadha [7] that showed, assuming the Gereralized Riemann Hypothsis, that $\pi_E^r(x) \ll x^{4/5}/(\log x)$.

3.4 Average Lang–Trotter

For every integer a, b such that $4a^3 + 27b^2 \neq 0$, we let

$$E(a,b) : y^2 = x^3 + ax + b.$$

We will conclude the lecture with a discussion of the following statement which appeared in [2]. Let r be an integer, $A, B > 1$. For every $c > 0$ we have

$$\frac{1}{4AB} \sum_{|a| \leq A, |b| \leq B} \pi_{E(a,b)}^r(x) = C_r \int_2^x \frac{dt}{\sqrt{t} \log t} + O\left(\left(\frac{1}{A} + \frac{1}{B} \right) x^{3/2} + \frac{x^{5/2}}{AB} + \frac{\sqrt{x}}{\log^c x} \right).$$

where

$$C_r = \frac{2}{\pi} \prod_\ell \frac{\# \operatorname{GL}_2(\mathbb{F}_\ell)_{\mathrm{tr}=r}}{\# \operatorname{GL}_2(\mathbb{F}_\ell)}.$$

References

[1] Cojocaru, Alina Carmen, *Cyclicity pf CM Elliptic Curves modulo p* Trans. of the AMS **355**, 7, (2003) 2651–2662.

[2] David, Chantal; Pappalardi, Francesco, *Average Frobenius Distribution of Elliptic Curves*, Internat. Math. Res. Notices **4** (1999) 165–183.

[3] Gupta, Rajiv; Murty M. Ram, *Primitive points on elliptic curves*, Compositio Mathematica **58**, n. 1 (1986), 13–44.

[4] Gupta, Rajiv; Murty M. Ram, *Cyclicity and generation of points mod p on elliptic curves*, Inventiones mathematicae **101** 1 (1990) 225–235

[5] Lang, Serge; Trotter, Hale, Frobenius distributions in GL_2-extensions. Lecture Notes in Mathematics, Vol. 504. *Springer-Verlag*, Berlin–New York, 1976

[6] Lang, Serge; Trotter, Hale, *Primitive points on elliptic curves.* Bull. Amer. Math. Soc. **83** (1977), no. 2, 289–292.

[7] Murty, M. Ram; Murty, V. Kumar; Saradha, N., *Modular Forms and the Chebotarev Density Theorem,* American Journal of Mathematics, **110**, No. 2 (1988), 253–281

[8] Serre, Jean-Pierre, Abelian ℓ-adic representations and elliptic curves. With the collaboration of Willem Kuyk and John Labute. Second edition. Advanced Book Classics. Addison-Wesley Publishing Company, *Advanced Book Program*, Redwood City, CA, 1989.

[9] Serre, Jean-Pierre, *Propriétés galoisiennes des points d'ordre fini des courbes elliptiques.* (French) Invent. Math. **15** (1972), no. 4, 259–331.

[10] Serre, Jean-Pierre, *Quelques applications du théorème de densité de Chebotarev.* (French) Inst. Hautes Études Sci. Publ. Math. No. **54** (1981), 323–401.