



Universiteit
Leiden
The Netherlands

Galois representations of elliptic curves and abelian entanglements

Brau Avila, Julio

Citation

Brau Avila, J. (2015, December 1). *Galois representations of elliptic curves and abelian entanglements*. Retrieved from <https://hdl.handle.net/1887/37019>

Version: Corrected Publisher's Version

License: [Licence agreement concerning inclusion of doctoral thesis in the Institutional Repository of the University of Leiden](#)

Downloaded from: <https://hdl.handle.net/1887/37019>

Note: To cite this publication please use the final published version (if applicable).

Cover Page



Universiteit Leiden



The handle <http://hdl.handle.net/1887/37019> holds various files of this Leiden University dissertation

Author: Brau Avila, Julio

Title: Galois representations of elliptic curves and abelian entanglements

Issue Date: 2015-12-01

Stellingen

behorende bij het proefschrift

*Galois Representations of elliptic curves
and abelian entanglements*

door **Julio Brau Avila**

1. Let $a, b \in \mathbb{Q}$ be rational numbers such that $E_{a,b} : Y^2 = X^3 + aX + b$ defines an elliptic curve that does not have complex multiplication over $\overline{\mathbb{Q}}$. Then there exists a deterministic algorithm which, given as inputs such a and b , determines the image of the Galois representation $\rho_{E_{a,b}}$ attached to the torsion points of $E_{a,b}$.
2. Let E/\mathbb{Q} be a Serre curve. Let D be the discriminant of $\mathbb{Q}(\sqrt{\Delta})$, where Δ is the discriminant of any Weierstrass model of E over \mathbb{Q} , and let C_E be the density (conditional on GRH) of primes p such that the group $\tilde{E}(\mathbb{F}_p)$ is cyclic. Then

$$C_E = \mathfrak{C}_E \prod_{\ell} \left(1 - \frac{1}{(\ell^2 - 1)(\ell^2 - \ell)} \right)$$

where the entanglement correction factor \mathfrak{C}_E is given by

$$\mathfrak{C}_E = \begin{cases} 1 & \text{if } D \equiv 0 \pmod{4} \\ 1 + \prod_{\ell|2D} \frac{-1}{(\ell^2 - 1)(\ell^2 - \ell) - 1} & \text{if } D \equiv 1 \pmod{4} \end{cases}$$

3. There exists a modular curve $X'(6)$ of level 6 defined over \mathbb{Q} whose \mathbb{Q} -rational points correspond to j -invariants of ellip-

tic curves E over \mathbb{Q} that satisfy $\mathbb{Q}(E[2]) \subset \mathbb{Q}(E[3])$, hence do not have abelian entanglements.

4. The modular curve $X'(6)$ completes a set \mathcal{X} of modular curves such that, for any elliptic curve E over \mathbb{Q} we have that

$$E \text{ is not a Serre curve} \iff j(E) \in \bigcup_{X \in \mathcal{X}} j(X(\mathbb{Q})).$$

5. Let E/\mathbb{Q} be the elliptic curve given by $Y^2 + XY + Y = X^3 - X^2 - X - 14$. Let $K = \mathbb{Q}(\zeta_3)$ and $L_m = K(\sqrt[3]{m})$. Then there are infinitely many cube-free m such that $\text{rk } E/L_m = 0$.

(J.Brau. Selmer groups of elliptic curves in degree p extensions, preprint. arxiv: 1401.3304, 2014.)

6. Suppose that G is a normal subgroup of $G_1 \times \cdots \times G_n$ such that the projection maps $\pi_i : G \rightarrow G_i$ are surjective for all i . Then the quotient $(G_1 \times \cdots \times G_n)/G$ is abelian.

7. Let E/\mathbb{Q} be the elliptic curve given by Weierstrass equation $Y^2 + Y = X^3 - X^2 - 10X - 20$. Then we expect $\tilde{E}(\mathbb{F}_p)$ to be cyclic for around 61% of primes p .

8. Let E be a non-CM elliptic curve over \mathbb{Q} and let S be the finite set of primes ℓ for which the representation $\rho_{E,\ell}$ is not surjective. Define

$$\begin{aligned} \mathcal{T} &:= \{2, 3\} \cup S \cup \{\ell : \ell \mid N_E\}, \\ m &:= \prod_{\ell \in \mathcal{T}} \ell. \end{aligned}$$

Then the integer m splits ρ_E , that is,

$$G = G_m \times \prod_{\ell \nmid m} \text{GL}_2(\mathbb{Z}_\ell).$$