Journal of Number Theory 168 (2016) 386–412

Contents lists available at ScienceDirect

Journal of Number Theory

www.elsevier.com/locate/jnt

An explicit open image theorem for products of elliptic curves

Davide Lombardo

Département de Mathématiques d'Orsay, France

ARTICLE INFO

Article history:
Received 29 November 2015
Received in revised form 15 March 2016
Accepted 5 April 2016
Available online 3 June 2016
Communicated by David Goss

MSC:
11F80
11G05
14K15
11G10

Keywords:
Elliptic curves
Galois representations
Open image theorem

ABSTRACT

Let K be a number field and let $E_1, \ldots, E_n$ be elliptic curves over K, pairwise non-isogenous over $\overline{K}$ and without complex multiplication over $\overline{K}$. We study the image G_∞ of the adelic representation of $\operatorname{Gal}\left(\overline{K}/K\right)$ naturally attached to $E_1 \times \cdots \times E_n$. The main result is an explicit bound for the index of G_∞ in $\left\{(x_1, \ldots, x_n) \in \operatorname{GL}_2(\hat{\mathbb{Z}})^n \;\middle|\; \det x_i = \det x_j \;\; \forall i, j\right\}$.

1. Introduction

In this work we prove an explicit, adelic surjectivity result for the Galois representation attached to a product of pairwise non-isogenous, non-CM elliptic curves, extending the result of [3]. Our main theorem is as follows:

E-mail address: davide.lombardo@math.u-psud.fr.

http://dx.doi.org/10.1016/j.jnt.2016.04.017

Theorem 1.1. *Let $E_1, \ldots, E_n$, $n \geq 2$, be elliptic curves defined over a number field K, pairwise not isogenous over $\overline{K}$. Suppose that $\operatorname{End}_{\overline{K}}(E_i) = \mathbb{Z}$ for $i = 1, \ldots, n$, and denote by G_∞ the image of $\operatorname{Gal}\left(\overline{K}/K\right)$ inside*

$$\prod_{i=1}^{n} \prod_{\ell} \operatorname{Aut}(T_\ell(E_i)) \cong \operatorname{GL}_2(\hat{\mathbb{Z}})^n.$$

Let $\gamma := 10^{13}$ and $\delta := \exp\exp\exp(12)$, and set

$$H = \max\left\{1, \log[K : \mathbb{Q}], \max_i h(E_i)\right\},$$

where $h(E_i)$ denotes the stable Faltings height of E_i. The group G_∞ has index at most

$$\delta^{n(n-1)} \cdot \left([K : \mathbb{Q}] \cdot H^2\right)^{\gamma n(n-1)}$$

in

$$\Delta := \left\{(x_1, \ldots, x_n) \in \operatorname{GL}_2(\hat{\mathbb{Z}})^n \;\middle|\; \det x_i = \det x_j \;\; \forall i, j\right\}.$$

Remark 1.2. Note that the compatibility of the Weil pairing with the action of Galois forces G_∞ to be contained in Δ. Also note that we shall prove slightly more precise statements (see Lemma 7.3 and Theorem 7.6 below), which immediately imply Theorem 1.1 by Proposition 2.7 and elementary estimates.

Let us give some context for our result. It has been known since the work of Serre and Masser–Wüstholz (cf. [7], Main Theorem and Proposition 1) that the isogeny theorem (section 2 below) gives an effective bound ℓ_0 on the largest prime ℓ for which the image of the representation

$$\operatorname{Gal}\left(\overline{K}/K\right) \to \operatorname{Aut}(T_\ell(E_1 \times \cdots \times E_n))$$

does not contain $\operatorname{SL}_2(\mathbb{Z}_\ell)^n$. As it was in [3], the main difficulty in proving Theorem 1.1 lies in controlling the image of the representation modulo powers of primes smaller than ℓ_0; in other words, the present result should be thought of as a bound on the exponent of any given prime appearing in the factorization of the index $[\Delta : G_\infty]$ (precise statements in this direction are obtained in section 6.2, cf. especially Proposition 6.12).

Besides the intrinsic interest of the question addressed by Theorem 1.1, notice that (by a standard argument similar to [3, Corollary 9.5]) our result gives a completely effective lower bound on the degree of the extension of K generated by a torsion point $(P_1, \ldots, P_n) \in E_1(\overline{K}) \times \cdots \times E_n(\overline{K})$ in terms of the order of P: such lower bounds can be useful in problems of “unlikely intersections”, see for example Masser’s survey [6], especially §7.