C. R. Acad. Sci. Paris, Ser. I 353 (2015) 1–4

Contents lists available at ScienceDirect

C. R. Acad. Sci. Paris, Ser. I

www.sciencedirect.com

Number theory

Base change for elliptic curves over real quadratic fields

Changement de base pour les courbes elliptiques sur les corps quadratiques réels

Luis Dieulefait [1], Nuno Freitas [2]

Mathematisches Institut, Universität Bayreuth, 95440 Bayreuth, Germany

ARTICLE INFO

Article history:
Received 17 July 2014
Accepted after revision 10 October 2014
Available online 30 October 2014

Presented by Jean-Pierre Serre

ABSTRACT

Let E be an elliptic curve over a real quadratic field K and F/K a totally real finite Galois extension. We prove that E/F is modular.

© 2014 Académie des sciences. Published by Elsevier Masson SAS. All rights reserved.

RÉSUMÉ

Soit E une courbe elliptique sur un corps quadratique réel K et F/K une extension totalement réele, finie et galoisienne. On demontre que E/F est modulaire.

© 2014 Académie des sciences. Published by Elsevier Masson SAS. All rights reserved.

1. Introduction

For F a totally real number field, we write $G_F := \mathrm{Gal}(\overline{\mathbb{Q}}/F)$ for its absolute Galois group. For a Hilbert modular form $\mathfrak{f}$, we denote by $\rho_{\mathfrak{f},\lambda}$ its attached λ-adic representation. We say that a continuous Galois representation $\rho : G_F \to \mathrm{GL}_2(\overline{\mathbb{Q}}_\ell)$ is *modular* if there exist a Hilbert newform $\mathfrak{f}$ and a prime $\lambda \mid \ell$ in its field of coefficients $\mathbb{Q}_{\mathfrak{f}}$ such that we have an isomorphism $\rho \sim \rho_{\mathfrak{f},\lambda}$. In [1] and [2, Section 5], the first named author proved a base change for the GL_2 case over $\mathbb{Q}$ [2, Theorem 1.2].

Theorem 1. *Let f be a classical modular form of weight $k \geq 2$ and field of coefficients $\mathbb{Q}_f$. For a prime λ of $\mathbb{Q}_f$, write $\rho_{f,\lambda}$ for the attached λ-adic representation. Let $F/\mathbb{Q}$ be a totally real number field. Then the Galois representation $\rho_{f,\lambda}|G_F$ is (Hilbert) modular in the sense above.*

In the recent paper [3], the following modularity theorem is proved.

Theorem 2. *Let E be an elliptic curve defined over a real quadratic field K. Then E is Hilbert modular over K.*

E-mail addresses: ldieulefait@ub.edu (L. Dieulefait), nunobfreitas@gmail.com (N. Freitas).

[1] The first-named author was supported by the MICINN Grant MTM2012-33830 and ICREA Academia Research Prize.

[2] The second-named author was supported through a grant within the framework of the DFG Priority Programme 1489 *Algorithmic and Experimental Methods in Algebra, Geometry and Number Theory* (grant number Sto 299/11-1).

http://dx.doi.org/10.1016/j.crma.2014.10.006

1631-073X/© 2014 Académie des sciences. Published by Elsevier Masson SAS. All rights reserved.

The aim of this note is to establish a base change result for certain elliptic curves as a consequence of Theorem 2. More precisely, we prove the following.

Theorem 3. *Let E be an elliptic curve over a real quadratic field K. Let also F/K be a totally real finite Galois extension. Then E/F is modular.*

This result has applications in the context of the Birch and Swinnerton–Dyer conjecture. Indeed, the modularity of E after base change guarantees that the L-function $L(E/F, s)$ is holomorphic in $\mathbb{C}$ and, in particular, its order of vanishing at $s = 1$ is a well-defined non-negative integer, in agreement with what is predicted by the BSD conjecture. Furthermore, the modularity of E/F allows the construction of Stark–Heegner points on E over (not necessarily real) quadratic extensions of F. For details regarding this application, we refer the reader to [4] and the references therein.

2. Elliptic curves with big non-solvable image mod $p = 3, 5$ or 7

Let F/K be a finite extension of totally real number fields. Let E/K be an elliptic curve. We will say that $\overline{\rho}_{E,p}(G_F)$ **is big** if $\overline{\rho}_{E,p}(G_{F(\zeta_p)})$ is absolutely irreducible, otherwise we say it **is small**. In particular, if $\overline{\rho}_{E,p}(G_F)$ is non-solvable, then it is big. We now restate [3, Theorems 3 and 4].

Theorem 4. *Let $p = 3, 5$ or 7. Let F/K and E/K be as above. Suppose that $\overline{\rho}_{E,p}(G_F)$ is big. Then E is modular over F.*

The following proposition is well-known.

Proposition 2.1. *Let F/K be a finite Galois extension of totally real fields and E/K an elliptic curve. Let p be a prime and suppose that $\overline{\rho}_{E,p}(G_K)$ is non-solvable. Then $\overline{\rho}_{E,p}(G_F)$ is non-solvable.*

Proof. Since $\overline{\rho}_{E,p}(G_K)$ is non-solvable, we have $p > 3$. From Dickson's theorem (see also Proposition 3.1), having $\overline{\rho}_{E,p}(G_K)$ non-solvable implies that projectively $\overline{\rho}_{E,p}(G_K)$ is A_5 or $\mathrm{PSL}_2(\mathbb{F}_p)$ or $\mathrm{PGL}_2(\mathbb{F}_p)$. For the last two cases, the proposition is a particular case of [1, Lemma 3.2]. Since A_5 is a simple group, the same argument as in [1, Lemma 3.2] also applies in this case. □

We have the following corollary.

Corollary 2.2. *Let F/K and E/K be as in Proposition 2.1. Let $p = 3, 5$ or 7. Suppose that $\overline{\rho}_{E,p}(G_K)$ is non-solvable. Then E is modular over F.*

Proof. From the previous proposition we have that $\overline{\rho}_{E,p}(G_F)$ is non-solvable, hence it is big. Thus E/F is modular by Theorem 4. □

3. Elliptic curves with projective image S_4 or A_4 mod $p = 3, 5$ or 7

Let E/K be an elliptic curve. We have seen that if $\overline{\rho}_{E,p}$ has a big non-solvable image, then after a base change to a totally real Galois extension its image is still non-solvable. We now want to understand what can happen when $\overline{\rho}_{E,p}(G_K)$ is big and solvable. We first recall the following well-know fact.

Proposition 3.1. *Let E/K be an elliptic curve. Write G for the image of $\overline{\rho}_{E,p}$ in $\mathrm{GL}_2(\mathbb{F}_p)$ and H for its image in $\mathrm{PGL}_2(\mathbb{F}_p)$. Then, there are the following possibilities:*

(a) *G is contained in a Borel subgroup;*
(b) *G contains $\mathrm{SL}_2(\mathbb{F}_p)$;*
(c) *H is cyclic, G is contained in a Cartan subgroup;*
(d) *H is dihedral, G is contained in the normalizer of a Cartan subgroup;*
(e) *H is isomorphic to A_4, S_4 or A_5.*

Let $p = 3, 5$ or 7. Let also G and H be as in the proposition. Remembering that $\mathrm{PSL}_2(\mathbb{F}_\ell)$ is simple for $p \geq 5$, by Jordan–Moore's theorem, and that $\mathrm{PSL}_2(\mathbb{F}_3) \simeq S_4$, we divide the cases where $\overline{\rho}_{E,p}(G_K)$ is big and solvable into two types:

(I) $H \cong S_4$ or A_4,
(II) H is dihedral.

Suppose we are in case (I). Let F/K be a finite Galois extension and set $H_F := \mathbb{P}(\overline{\rho}_{E,p}(G_F))$. We would like that H_F to be also isomorphic to A_4 or S_4, since this would mean that $\overline{\rho}_{E,p}(G_F)$ is big and Theorem 4 applies. Since F/K is Galois, we have that H_F is a normal subgroup of H. Write $I = \{1\}$ for the trivial group and D_4 for the dihedral group in four elements. The normal subgroups of S_4 and A_4 are respectively

- I, D_4, A_4 and S_4,
- I, D_4 and A_4.

Thus, the cases where Theorem 4 does not apply over F are when the pair of groups (H, H_F) is one of

$$(S_4, D_4), \quad (S_4, I), \quad (A_4, D_4), \quad (A_4, I). \tag{1}$$

Since we are working with totally real fields, the complex conjugation has projective image of order 2. Thus the cases with $H_F = I$ cannot happen.

3.1. A Sylow base change

We now deal with the remaining cases from (1). Recall that we want to base change E/K to F where F/K is finite and Galois. Suppose that (H, H_F) is (S_4, D_4) or (A_4, D_4). Let F_3 be a subfield of F such that the Galois group $\mathrm{Gal}(F/F_3)$ is a 3-Sylow subgroup of $\mathrm{Gal}(F/K)$. In particular, F/F_3 is a solvable extension. We shall shortly prove the following.

Lemma 3.2. *The projective image $H_{F_3} := \mathbb{P}(\overline{\rho}_{E,p}(G_{F_3}))$ is isomorphic to S_4 or A_4. In particular, $\overline{\rho}_{E,p}(G_{F_3})$ is big.*

From this lemma and Theorem 4, it follows that E/F_3 is modular. Finally, an application of Langlands solvable base change (see [6]) allows us to conclude that E/F is modular.

For the proof of Lemma 3.2, we will need the following elementary lemma from group theory.

Lemma 3.3. *Let G be a profinite group. Let $M \subset G$ be a subgroup of finite index i. Let N be a normal subgroup of G. Write j for the index of $M/(N \cap M)$ in G/N. Then $j \mid i$.*

Proof. We prove it for the case of finite groups. The required divisibility follows from the following elementary equalities:

$$|G| = |N| \cdot [G : N],$$

$$|M| = |N \cap M| \cdot [M : N \cap M].$$

Dividing the first equality into the second, we conclude that j divides i. □

Proof of Lemma 3.2. Let F_3 be as above and set

$$G := \mathrm{Gal}(\overline{\mathbb{Q}}/K), \qquad M := \mathrm{Gal}(\overline{\mathbb{Q}}/F_3), \qquad N := \mathrm{Ker}(\mathbb{P}\overline{\rho}_{E,p}).$$

Let L/K be the Galois extension fixed by N. Observe that $L/L \cap F_3$ is Galois and

$$G/N \cong \mathrm{Gal}(L/K), \qquad M/(M \cap N) \cong \mathrm{Gal}(L/L \cap F_3).$$

From Lemma 3.3, we see that

$$\big[\mathrm{Gal}(L/K) : \mathrm{Gal}(L/L \cap F_3)\big] = j \mid i = [G : M]$$

and we also have

$$\big|\mathrm{Gal}(L/K)\big| = j\big|\mathrm{Gal}(L/L \cap F_3)\big|.$$

Note that $\mathrm{Gal}(L/L \cap F_3) \cong H_{F_3}$. From the way we choose F_3 it is clear that $3 \nmid i$, hence $3 \nmid j$. By hypothesis $G/N \cong S_4$ or A_4, hence 3 divides $|\mathrm{Gal}(L/K)|$ and $|H_{F_3}|$. Finally, the conditions $3 \mid |H_{F_3}|$ and $D_4 \subset H_{F_3}$ together imply that H_{F_3} is isomorphic to S_4 or A_4. □

We summarize this section into the following corollary.

Corollary 3.4. *Let F/K be a finite Galois extension of totally real fields. Let E/K be an elliptic curve. Suppose that for $p = 3, 5$ or 7 we have that $\overline{\rho}_{E,p}(G_K)$ is big and solvable. Suppose further that $\mathbb{P}(\overline{\rho}_{E,p}(G_K)) \cong S_4$ or A_4. Then E/F is modular.*

Everything we have done so far works for any Galois extension F/K. Moreover, it is clear that the remaining cases are those when $\overline{\rho}_{E,p}(G_K)$ is small or projectively dihedral simultaneously for $p = 3, 5, 7$. The restriction in the statement of Theorem 3 to quadratic fields arises precisely from dealing with them, which is the content of the next section.

4. Elliptic curves having small or projective Dihedral image at $p = 3, 5$ and 7

Let K be a real quadratic field. From Theorem 4 an elliptic curve E/K is modular over K except possibly if $\bar{\rho}_{E,p}(G_K)$ is small simultaneously for $p = 3, 5, 7$. Suppose $K \neq \mathbb{Q}(\sqrt{5})$. In [3], it is shown that such an elliptic curve gives rise to a K-point on one of the following modular curves:

$$X(\mathrm{b5}, \mathrm{b7}), \quad X(\mathrm{b3}, \mathrm{s5}), \quad X(\mathrm{s3}, \mathrm{s5}),$$

$$X(\mathrm{b3}, \mathrm{b5}, \mathrm{d7}), \quad X(\mathrm{s3}, \mathrm{b5}, \mathrm{d7}), \quad X(\mathrm{b3}, \mathrm{b5}, \mathrm{e7}), \quad X(\mathrm{s3}, \mathrm{b5}, \mathrm{e7}),$$

where b and s respectively stand for 'Borel' and 'normalizer of split Cartan'. The notation d7 and e7 is explained in [3, Section 10]; here we remark only that they indicate mod 7 level structures that are respectively finer than 'normalizer of split Cartan' and 'normalizer of non-split Cartan'. Denote by $\mathcal{E}_K$ the set of elliptic curves (up to quadratic twist) corresponding to K-points in the previous modular curves. In [3] it is also shown that an elliptic curve $E/\mathbb{Q}(\sqrt{5})$ with simultaneously small image for $p = 3, 5, 7$ gives rise to a $\mathbb{Q}(\sqrt{5})$-point in one of the following modular curves:

$$X(\mathrm{d7}), \quad X(\mathrm{e7}), \quad X(\mathrm{b3}, \mathrm{b7}), \quad X(\mathrm{s3}, \mathrm{b7}).$$

Denote by $\mathcal{E}_{\mathbb{Q}(\sqrt{5})}$ the set of elliptic curves (up to quadratic twist) corresponding to $\mathbb{Q}(\sqrt{5})$-points in these four modular curves.

Furthermore, it also follows from [3] that, for any real quadratic field K, we have:

(i) $\mathcal{E}_K$ contains all elliptic curves (up to quadratic twist) with small or projective dihedral image simultaneously at $p = 3, 5, 7$;
(ii) $\mathcal{E}_K$ is finite;
(iii) let $E \in \mathcal{E}_K$. Then, either E is a $\mathbb{Q}$-curve or E has complex multiplication or $\bar{\rho}_{E,7}(G_K)$ contains $\mathrm{SL}_2(\mathbb{F}_7)$.

We can now easily prove the following.

Corollary 4.1. *Let K be a real quadratic field. Let $E \in \mathcal{E}_K$. Let F/K be a finite totally real Galois extension. Then E/F is modular.*

Proof. From (iii) above, we know that either (a) E/K is a $\mathbb{Q}$-curve or has complex multiplication or (b) $\bar{\rho}_{E,7}(G_K)$ is non-solvable. Suppose we are in case (a). Base change follows from [5, Proposition 12.1] in the CM case; if E is a $\mathbb{Q}$-curve, by results of Ribet and Serres' conjecture (now a theorem due to Khare–Wintenberger), it arises from a classical modular form thus base change follows by Theorem 1. In case (b), it follows from Corollary 2.2 that E/F is modular. □

5. Proof of the main theorem

Let K be a real quadratic field and E/K an elliptic curve. Write $\bar{\rho}_p = \bar{\rho}_{E,p}$. The curve E/K must satisfy at least one of the following three cases:

(1) $\bar{\rho}_p(G_K)$ is big and non-solvable for some $p \in \{3, 5, 7\}$,
(2) $\bar{\rho}_p(G_K)$ is big, solvable and satisfy $\mathbb{P}(\bar{\rho}_p(G_K)) \cong S_4, A_4$ for some $p \in \{3, 5, 7\}$,
(3) E/K belongs to the set $\mathcal{E}_K$.

Let F/K be a totally real finite Galois extension. In each case, modularity of E/F now follows directly from one of the previous sections:

Case (1): this is Corollary 2.2.
Case (2): this is Corollary 3.4.
Case (3): this is Corollary 4.1. □

Acknowledgements

We would like to thank Kęstutis Česnavičius, José María Giral, Victor Rotger and Samir Siksek for their useful comments. We also thank the anonymous referee for his comments.

References

[1] L. Dieulefait, Langlands base change for GL(2), Ann. Math. 176 (2012) 1015–1038.
[2] L. Dieulefait, Automorphy of $\mathrm{Symm}^5(GL(2))$ and base change (with Appendix A by R. Guralnick and Appendix B by L. Dieulefait and T. Gee), submitted for publication, http://arxiv.org/abs/1208.3946.
[3] N. Freitas, B.V. Le Hung, S. Siksek, Elliptic curves over real quadratic fields are modular, Invent. Math. (2014), http://dx.doi.org/10.1007/s00222-014-0550-z, in press.
[4] X. Guitart, V. Rotger, Y. Zhao, Almost totally complex points on elliptic curves, Trans. Amer. Math. Soc. 336 (2014) 2773–2802.
[5] H. Jacquet, R.P. Langlands, Automorphic Forms on GL(2), Lect. Notes Math., vol. 114, Springer-Verlag, Berlin, 1970.
[6] R.P. Langlands, Base Change for GL(2), Ann. Math. Stud., vol. 96, 1980.