# ON THE MODULARITY LEVEL OF MODULAR ABELIAN VARIETIES OVER NUMBER FIELDS

ENRIQUE GONZÁLEZ–JIMÉNEZ AND XAVIER GUITART

ABSTRACT. Let f be a weight two newform for  $\Gamma_1(N)$  without complex multiplication. In this article we study the conductor of the absolutely simple factors B of the variety  $A_f$  over certain number fields L. The strategy we follow is to compute the restriction of scalars  $\operatorname{Res}_{L/\mathbb{Q}}(B)$ , and then to apply Milne's formula for the conductor of the restriction of scalars. In this way we obtain an expression for the local exponents of the conductor  $\mathcal{N}_L(B)$ . Under some hypothesis it is possible to give global formulas relating this conductor with N. For instance, if N is squarefree we find that  $\mathcal{N}_L(B)$  belongs to  $\mathbb{Z}$  and  $\mathcal{N}_L(B) \mathfrak{f}_L^{\dim B} = N^{\dim B}$ , where  $\mathfrak{f}_L$  is the conductor of L.

### 1. INTRODUCTION

Let C be an elliptic curve defined over  $\mathbb{Q}$ . The Shimura-Taniyama-Weil conjecture, also known as the modularity theorem after its proof by Wiles et al. [15, 3] asserts that there exists a surjective morphism  $J_0(N) \to C$  defined over  $\mathbb{Q}$ , where  $J_0(N)$  is the Jacobian of the modular curve  $X_0(N)$ . Moreover, the minimum N with this property is equal to  $\mathcal{N}_{\mathbb{Q}}(C)$ , the conductor of C.

A generalization of the modularity theorem, which as Ribet showed in [12] is a consequence of the recently proved Serre's conjecture on residual Galois representations, characterizes the modular abelian varieties over  $\mathbb{Q}$ ; that is, the  $\mathbb{Q}$ -simple abelian varieties A defined over  $\mathbb{Q}$  with a surjective morphism  $J_1(N) \rightarrow A$ . They are the so-called (simple) varieties of GL<sub>2</sub>-type: those whose endomorphism algebra  $\mathbb{Q} \otimes \operatorname{End}_{\mathbb{Q}}(A)$  is a number field of degree over  $\mathbb{Q}$  equal to dim A.

From the modular form side, one can start with a weight two newform f for  $\Gamma_1(N)$ . A construction of Shimura attaches to such an f an abelian variety  $A_f$  over  $\mathbb{Q}$ , which is a quotient of  $J_1(N)$ ; in fact, all quotients of  $J_1(N)$  over  $\mathbb{Q}$  are of this form. For these varieties Carayol [5] proved that  $\mathcal{N}_{\mathbb{Q}}(A_f) = N^{\dim A_f}$ . The generalization of Shimura-Taniyama-Weil asserts that each abelian variety of GL<sub>2</sub>-type is isogenous over  $\mathbb{Q}$  to an  $A_f$  for some f, therefore the formula  $\mathcal{N}_{\mathbb{Q}}(A) = N^{\dim A}$  is valid for all A of GL<sub>2</sub>-type.

The modular abelian varieties  $A_f$  are simple over  $\mathbb{Q}$ , but they are not absolutely simple in general: they are isogenous over  $\overline{\mathbb{Q}}$  to a power of an absolutely simple variety, which is called a building block for  $A_f$ . To be more precise, if L is the smallest number field where all the endomorphisms of  $A_f$  are defined, then  $A_f$  is isogenous over L to a variety of the form  $B^n$ , for some absolutely simple variety

Date: November 10, 2021.

The first author was supported in part by grants MTM 2009-07291 (Ministerio de Educación y Ciencia, Spain) and CCG08-UAM/ESP-3906 (Universidad Autonóma de Madrid-Comunidad de Madrid, Spain). The second author was supported in part by grants 2009 SGR 1220 and MTM2009-13060-C02-01.

*B* defined over *L*. In this article we discuss possible generalizations of Carayol's formula for these modular abelian varieties over number fields B/L, in the case where they do not have CM.

More concretely, in section 2 we recall the notation and basic facts regarding modular abelian varieties and building blocks. Afterwards, we give the explicit decomposition of the restriction of scalars  $\operatorname{Res}_{L/\mathbb{Q}}(B)$  as as product of modular abelian varieties up to isogeny over  $\mathbb{Q}$ . We use this in section 3 in order to give an expression for the local exponents of  $\mathcal{N}_L(B)$ , in terms of the levels of certain twists of f by Dirichlet characters related to the field L. In some cases, the conductor  $\mathcal{N}_L(B)$  turns out to be a rational integer and we obtain similar formulas to the ones for the varieties  $A_f$ ; we remark that in this situation the conductor of L, that we denote by  $\mathfrak{f}_L$ , also appears in the expressions. We have collected all these formulas, that appear in the text as propositions 8, 10 and 11, in the following

**Main Theorem.** Let  $f \in S_2(N, \varepsilon)$  be a weight two newform for  $\Gamma_1(N)$  with Nebentypus  $\varepsilon$  and without complex multiplication. Let  $A_f$  be the modular abelian variety attached to f, let L be the smallest field of definition of the endomorphisms of  $A_f$ , and let B/L be a simple quotient of  $A_f$  over L.

- (1) Suppose that one of the following conditions is satisfied:
  - N is odd and  $\operatorname{ord}(\varepsilon) \leq 2$ ,
  - N is squarefree.

Then  $\mathcal{N}_L(B)$  belongs to  $\mathbb{Z}$  and

$$\mathcal{N}_L(B)\,\mathfrak{f}_L^{\dim B}=N^{\dim B}.$$

- (2) If f is a newform for  $\Gamma_0(N)$ , that is if  $\varepsilon = 1$ , then  $\mathcal{N}_L(B)$  belongs to  $\mathbb{Z}$ . Moreover,
  - (a) if  $v_2(\mathfrak{f}_L) = 3$  and  $v_2(\mathfrak{f}_K) = 2$  for some  $K \subseteq L$  then

 $2 \mathcal{N}_L(B) \mathfrak{f}_L^{\dim B} = N^{\dim B}$ 

(b) in the remaining cases for L then

$$\mathcal{N}_L(B) \mathfrak{f}_L^{\dim B} = N^{\dim B}.$$

Finally, in section 4 we provide some examples of building blocks of dimension one and two with their corresponding equations. Concretely, for the case of dimension one we compute their conductors, in order to show the different behaviors when the hypothesis of the above theorem are not satisfied. We observe that, although the conductor can be a rational integer sometimes, formulas as the ones in the theorem do not always hold; we also give examples where the conductor is not a rational integer. For the case of dimension two, the level-conductors local formula provided at Proposition 5 allows us to compute the conductor of the Jacobian of a genus two curve defined over a number field that corresponds to a building block.

#### 2. Modular Abelian Varieties

We begin this section by recalling the basic facts about modular abelian varieties and their absolutely simple factors that we will use. In particular, we introduce the type of varieties that we will be dealing with in the rest of the article: the building blocks. Our goal is to prove a formula for the restriction of scalars of building blocks, which will be the base for our analysis of their conductors in the subsequent sections. Let  $f = \sum a_n q^n \in S_2(N, \varepsilon)$  be a normalized newform without complex multiplication of weight 2, level N and Nebentypus  $\varepsilon$ , and let  $E = \mathbb{Q}(\{a_n\})$  and  $F = \mathbb{Q}(\{a_p^2 \varepsilon(p)^{-1}\}_{p \nmid N})$ . These number fields will be denoted by  $E_f$  and  $F_f$  if we need to make the newform from which they come from explicit. The extension E/Fis abelian, and for each  $s \in \operatorname{Gal}(E/F)$  there exists a single Dirichlet character  $\chi_s$ such that  ${}^s f = f \otimes \chi_s$ , where  $f \otimes \chi_s$  is a newform whose p-th Fourier coefficient coincides with  $a_p \chi_s(p)$  for almost all p (see [11, §3 ]). Since  ${}^s f$  has level N, the conductor of  $\chi_s$  is divisible only by primes dividing N. We will also consider another number field attached to f, namely  $L = \overline{\mathbb{Q}}^{\cap \ker \chi_s}$  where s runs through  $\operatorname{Gal}(E/F)$ .

Shimura [13, Theorem 1] attached to f an abelian variety  $A_f/\mathbb{Q}$  constructed as a quotient of  $J_1(N)$ , the Jacobian of the modular curve  $X_1(N)$ , and with an action of E as endomorphisms defined over  $\mathbb{Q}$ . In fact,  $\mathbb{Q} \otimes_{\mathbb{Z}} \operatorname{End}_{\mathbb{Q}}(A_f) \simeq E$  and since dim  $A_f = [E : \mathbb{Q}]$ , the modular abelian varieties  $A_f$  are of GL<sub>2</sub>-type; as a consequence of Serre's conjecture all varieties of GL<sub>2</sub>-type are isogenous to some  $A_f$ .

The variety  $A_f$  is simple over  $\mathbb{Q}$ , but it is not necessarily absolutely simple. In general,  $A_f$  is isogenous over  $\overline{\mathbb{Q}}$  to a power of an absolutely simple abelian variety B, which is called a *building block* of  $A_f$ . This B has some remarkable properties; for instance, it is isogenous to all of its Galois conjugates. In addition, its endomorphism algebra  $\mathbb{Q} \otimes \text{End}(B)$  is a central division algebra over a number field isomorphic to F, it has Schur index t = 1 or t = 2 and its reduced degree  $t[F:\mathbb{Q}]$  is equal to dim B. The building blocks of dimension one are the  $\mathbb{Q}$ -curves, i.e. the elliptic curves  $B/\overline{\mathbb{Q}}$  that are isogenous to all of their Galois conjugates.

There are infinitely many varieties  $A_f$  with the same absolutely simple factor up to isogeny. However, by a result of Ribet [11, Theorem 4.7] if this happens for two varieties  $A_f$  and  $A_g$  we can suppose that g is the twist of f by some Dirichlet character. We will need a more precise version of this result, which already appears implicitly in Ribet's proof.

**Proposition 1.** Let f, g be two normalized newforms without complex multiplication such that  $A_f \sim_K B^n$  and  $A_g \sim_K B^m$  for some absolutely simple abelian variety B over a number field K. Then there exists a character  $\chi : \operatorname{Gal}(K/\mathbb{Q}) \to \mathbb{C}^{\times}$  such that  $g = f \otimes \chi$ .

Proof. Let  $V_f = T_\ell(A_f) \otimes \mathbb{Q}$  and  $V_g = T_\ell(A_g) \otimes \mathbb{Q}$ , where  $T_\ell(A_f)$  and  $T_\ell(A_g)$  are the Tate modules attached to  $A_f$  and  $A_g$  respectively, and let  $H = \operatorname{Gal}(\overline{\mathbb{Q}}/K)$ . Under the hypothesis of the proposition we have  $\operatorname{Hom}_H(V_f, V_g) \neq 0$ . By [11, Theorem 4.7], there exists a character  $\chi : G_{\mathbb{Q}} \to \mathbb{C}^{\times}$  such that  $f = g \otimes \chi$ . Ribet already asserts in the proof of his theorem that  $\chi$  is necessarily trivial on H. Therefore,  $\chi$  comes from a character  $\chi : \operatorname{Gal}(K/\mathbb{Q}) \to \mathbb{C}^{\times}$ .

González and Lario proved in [8] that L is the smallest number field where all the endomorphisms of  $A_f$  are defined. This implies that  $A_f \sim_L B^n$ , with B/L a building block with the endomorphisms defined over L and which is L-isogenous to all of its Galois conjugates. From now on B will denote such a building block obtained by decomposing  $A_f$  over the field L defined above, and t will denote the Schur index of End(B). Using the results in [7] one can show that the restriction of scalars  $\operatorname{Res}_{L/\mathbb{Q}}(B)$  is isogenous over  $\mathbb{Q}$  to a product of modular abelian varieties. Indeed, one has the following **Proposition 2.** The restriction of scalars  $\operatorname{Res}_{L/\mathbb{Q}}(B)$  decomposes into simple abelian varieties up to isogeny as

(1) 
$$\operatorname{Res}_{L/\mathbb{Q}}(B) \sim_{\mathbb{Q}} \prod \left(A_{f_1}\right)^t \times \cdots \times \left(A_{f_r}\right)^t,$$

where  $A_{f_1}, \ldots, A_{f_r}$  are non-isogenous modular abelian varieties.

Proof. There exists a map  $\alpha$ :  $\operatorname{Gal}(L/\mathbb{Q}) \to E^{\times}$  such that  ${}^{\sigma}\varphi = \alpha(\sigma) \circ \varphi \circ \alpha(\sigma)^{-1}$ . The  $\alpha(\sigma)$  can be identified with an element of  $\mathbb{Q} \otimes \operatorname{End}_{\mathbb{Q}}(A_f)$ , and together with an isogeny  $A_f \sim_L B^n$  it can be used to construct an isogeny  $\mu_{\sigma} \colon {}^{\sigma}B \to B$  compatible with  $\operatorname{End}(A_f)$  (see [10, Proposition 1.5]). It turns out that  $\mu_{\sigma} \circ {}^{\sigma}\mu_{\tau} \circ \mu_{\sigma\tau}^{-1} = \alpha(\sigma) \circ \alpha(\tau) \circ \alpha(\sigma\tau)^{-1}$  as elements of the center of  $\mathbb{Q} \otimes \operatorname{End}(B)$ . Therefore, the cocycle  $c_{B/L}(\sigma, \tau) = \mu_{\sigma} \circ {}^{\sigma}\mu_{\tau} \circ \mu_{\sigma\tau}^{-1}$  is symmetric, since  $\operatorname{Gal}(L/\mathbb{Q})$  is abelian. Now [7, Theorem 5.3] implies that  $\operatorname{Res}_{L/\mathbb{Q}}(B)$  is isogenous over  $\mathbb{Q}$  to a product  $A_1^{n_1} \times \cdots \times A_r^{n_r}$ , where the  $A_i$  are non-isogenous abelian varieties of  $\operatorname{GL}_2$ -type. But each of these varieties of  $\operatorname{GL}_2$ -type  $A_i$  is isogenous to some modular abelian variety  $A_{f_i}$ , and by [7, Lemma 5.1] each  $n_i$  is equal to t.

The rest of the section is devoted to give an explicit expression for the modular forms that appear in (1), in terms of a certain action of  $\operatorname{Gal}(E/F)$  on a group of characters that we now define. For  $s \in \operatorname{Gal}(E/F)$  let  $\chi_s$  be the Galois character such that  ${}^sf = f \otimes \chi_s$ , and let  $G \subseteq \operatorname{Hom}(G_{\mathbb{Q}}, \mathbb{C}^{\times})$  be the group generated by all such  $\chi_s$ . Since L is the fixed field of  $\overline{\mathbb{Q}}$  by  $\cap_s \ker \chi_s$ , it is also the fixed field of  $\overline{\mathbb{Q}}$  by  $\cap_{\chi \in G} \ker \chi$ . However, we remark that a character  $\chi \in G$  is not necessarily of the form  $\chi_s$ , but a product of elements of the form  $\chi_s$  in general. An element  $\chi \in G$  is trivial when restricted to  $\operatorname{Gal}(\overline{\mathbb{Q}}/L)$ , so it can be identified with a character  $\operatorname{Gal}(L/\mathbb{Q}) \to \mathbb{C}^{\times}$ . In fact, G can be identified with  $\operatorname{Hom}(\operatorname{Gal}(L/\mathbb{Q}), \mathbb{C}^{\times})$  and therefore we have that  $|G| = [L: \mathbb{Q}]$  (cf. [14, pp. 21-22]). We define an action of  $\operatorname{Gal}(E/F)$  on G by

$$\begin{array}{cccc} \operatorname{Gal}(E/F) \times G & \longrightarrow & G \\ (s,\chi) & \longmapsto & s \cdot \chi = \chi_s{}^s \chi. \end{array}$$

The cocycle identity of the characters  $\chi_s$  ([11, Proposition 3.3]) implies that it is indeed a group action, since for  $s, t \in \text{Gal}(E/F)$  we have that  $s \cdot (t \cdot \chi) = s \cdot (\chi_t^{t} \chi) = \chi_s^{s} \chi_t^{st} \chi = \chi_{st}^{st} \chi = (st) \cdot \chi$ . Let  $\hat{G}$  be a system of representatives for the orbits of G, and for  $\chi \in G$  let  $I_{\chi}$  be the isotropy subgroup of G at  $\chi$ .

Lemma 3. dim
$$(A_{f\otimes\chi}) \leq [\operatorname{Gal}(E/F):I_{\chi}][F:\mathbb{Q}]$$

*Proof.* For  $s \in \operatorname{Gal}(E/F)$  the character  $\chi_s$  takes values in E, since  $\chi_s(p) = {}^sa_p/a_p$  for almost all p. Therefore, any  $\chi \in G$  also takes values in E. This implies that  $E_{f\otimes\chi}$ , the field of Fourier coefficients of  $f\otimes\chi$ , is contained in E. For any  $s \in I_{\chi}$  we have that  ${}^s(f\otimes\chi) = {}^sf\otimes{}^s\chi = f\otimes\chi_s{}^s\chi_s = f\otimes(s\cdot\chi) = f\otimes\chi$ . By Galois theory we find that  $I_{\chi} \subseteq \operatorname{Gal}(E/E_{f\otimes\chi})$  and so  $|I_{\chi}| \leq [E:\mathbb{Q}]/[E_{f\otimes\chi}:\mathbb{Q}]$ , which gives that

$$\dim(A_{f\otimes\chi}) = [E_{f\otimes\chi}:\mathbb{Q}] \leqslant \frac{[E:\mathbb{Q}]}{\mid I_{\chi}\mid} = \frac{[E:F]}{\mid I_{\chi}\mid} [F:\mathbb{Q}] = [\operatorname{Gal}(E/F):I_{\chi}][F:\mathbb{Q}].$$

Now we can give explicitly the modular forms appearing in proposition 2, and we can also give the dimension of the corresponding modular abelian varieties. **Proposition 4.** The inequality in lemma 3 is in fact an equality and

(2) 
$$\operatorname{Res}_{L/\mathbb{Q}}(B) \sim_{\mathbb{Q}} \prod_{\chi \in \hat{G}} \left(A_{f \otimes \chi}\right)^t.$$

Proof. Let  $A = \operatorname{Res}_{L/\mathbb{Q}} B$ . Since B is L-isogenous to all of its Galois conjugates and  $A \simeq_L \prod_{\sigma \in \operatorname{Gal}(L/\mathbb{Q})} {}^{\sigma}B$ , we have that A is L-isogenous to  $B^{[L:\mathbb{Q}]}$ . Therefore, if  $A_g$  is a simple factor of A over  $\mathbb{Q}$  it isogenous to a power of B over L. Since  $A_f$  is also isogenous to a power of B over L, proposition 1 implies that  $g = f \otimes \chi$  for some Galois character  $\chi \in G$ . Hence, the modular forms  $f_i$  of the decomposition (1) are of the form  $f \otimes \chi$  for some  $\chi$  belonging to G. But if  $\chi, \chi' \in G$  are in the same orbit for the action of  $\operatorname{Gal}(E/F)$ , the varieties  $A_{f \otimes \chi}$  and  $A_{f \otimes \chi'}$  are isogenous over  $\mathbb{Q}$ . Indeed, in this case  $s \cdot \chi = \chi'$  for some  $s \in \operatorname{Gal}(E/F)$ , and then  ${}^s(f \otimes \chi) = f \otimes \chi'$ . This, together with the fact that the modular abelian variety attached to  ${}^s(f \otimes \chi)$ is isogenous over  $\mathbb{Q}$  to the one attached to  $f \otimes \chi$  implies that  $A_{f \otimes \chi}$  is isogenous to  $A_{f \otimes \chi'}$  over  $\mathbb{Q}$ .

Therefore, proposition 2 implies that there exists an exhaustive morphism over  $\mathbb Q$ 

$$\lambda \colon \prod_{\chi \in \hat{G}} \left( A_{f \otimes \chi} \right)^t \longrightarrow A,$$

so we have that

$$t[F:\mathbb{Q}]|G| = |G|\dim B = \dim A \leqslant \sum_{\chi \in \hat{G}} \dim (A_{f \otimes \chi})^t$$
$$\leqslant \quad t[F:\mathbb{Q}] \sum_{\chi \in \hat{G}} [\operatorname{Gal}(E/F):I_{\chi}] = t[F:\mathbb{Q}]|G|.$$

We see that each inequality is in fact an equality, and  $\lambda$  is an isogeny since the dimensions of the source and the target are the same.

#### 3. Level-conductors formulas

As in the previous section we consider a newform  $f \in S_2(N, \varepsilon)$  and a decomposition  $A_f \sim_L B^n$  of  $A_f$  into a power of a building block B defined over the field L, and we continue with the same notation as before with respect to the endomorphism algebra of B; namely, F is its center and t its Schur index. In this section we use the decomposition (2) to compute the local exponent of the conductor of B. In some particular cases we prove that the conductor belongs to  $\mathbb{Z}$  (i.e. it is a principal ideal generated by a rational integer), and we are able to give a global formula for it involving the conductor of L and the level of f. We denote by  $\mathcal{N}_L(B)$ the conductor of B over L, by  $\mathfrak{f}_L$  the conductor of L and by  $N_{L/\mathbb{Q}}$  the norm in the extension  $L/\mathbb{Q}$ . If  $\chi$  is a character belonging to G, we also denote by  $\mathcal{N}_{\chi}$  the level of the newform  $f \otimes \chi$  and by  $\mathfrak{f}_{\chi}$  the conductor of  $\chi$ . For a prime q,  $v_q(x)$  denotes the valuation of x at q and  $\chi_q$  the q-primary component of  $\chi$ .

**Proposition 5.** For each rational prime q we have that

(3) 
$$v_q(N_{L/\mathbb{Q}}(\mathcal{N}_L(B))) + 2(\dim B) \sum_{\chi \in G} v_q(\mathfrak{f}_{\chi}) = (\dim B) \sum_{\chi \in G} v_q(N_{\chi}).$$

*Proof.* By applying the formula of [9, Proposition 1] for the conductor of the restriction of scalars to (2) we obtain that

$$N_{L/\mathbb{Q}}\left(\mathcal{N}_{L}(B)\right)\left(d_{L/\mathbb{Q}}\right)^{2\dim B} = \prod_{\chi \in \hat{G}} \mathcal{N}_{\mathbb{Q}}\left(A_{f \otimes \chi}\right)^{t},$$

where  $d_{L/\mathbb{Q}}$  is the discriminant of  $L/\mathbb{Q}$ . By a theorem of Carayol ([5]) the conductor of a modular abelian variety  $A_g$  is  $N_g^{\dim A_g}$ , where  $N_g$  is the level of the newform g. Using this property and the conductor-discriminant formula (cf. [14, p. 28]) we find that

$$N_{L/\mathbb{Q}}\left(\mathcal{N}_{L}(B)\right)\prod_{\chi\in G}(\mathfrak{f}_{\chi})^{2\dim B}=\prod_{\chi\in \hat{G}}N_{\chi}^{t[\operatorname{Gal}(E/F):I_{\chi}][F:\mathbb{Q}]}.$$

But  $t[F:\mathbb{Q}] = \dim B$ , and the orbit of  $\chi$  contains  $[\operatorname{Gal}(E/F): I_{\chi}]$  elements, each one giving a modular abelian variety of the same dimension. Thus we have that

$$N_{L/\mathbb{Q}}\left(\mathcal{N}_{L}(B)\right)\prod_{\chi\in G}(\mathfrak{f}_{\chi})^{2\dim B}=\prod_{\chi\in G}N_{\chi}^{\dim B}$$

from which (3) follows by taking valuations at q.

Each prime  $\mathfrak{q}$  dividing q appears in  $\mathcal{N}_L(B)$  with the same exponent (see the proof of lemma 7). This observation together with (3) gives a way of computing the local exponents of  $\mathcal{N}_L(B)$  in terms of the levels  $N_{\chi}$ . In almost all cases [1, Theorem 3.1] can be used to compute the levels of the twisted newforms. Under some hypothesis one can also perform directly the computation, as in the following:

**Lemma 6.** If  $\operatorname{ord}(\varepsilon) \leq 2$  then for all primes  $q \neq 2$  we have that

(4) 
$$v_q(N_{L/\mathbb{Q}}(\mathcal{N}_L(B))) + [L:\mathbb{Q}](\dim B) v_q(\mathfrak{f}_L) = [L:\mathbb{Q}](\dim B) v_q(N).$$

*Proof.* First of all suppose that  $v_q(\mathfrak{f}_L) = 0$ . Then for each  $\chi \in G$  we have that  $v_q(\mathfrak{f}_{\chi}) = 0$  and (4) follows from (3) since  $v_q(N_{\chi}) = v_q(N)$  for all  $\chi \in G$  and  $|G| = [L:\mathbb{Q}]$ .

Suppose now that  $v_q(\mathfrak{f}_L) \neq 0$ . This means that there exists an element  $s \in \operatorname{Gal}(E/F)$  such that  $v_q(\mathfrak{f}_{\chi_s}) \neq 0$ . But  $\chi_s$  is a quadratic character since the relation  ${}^sf = f \otimes \chi_s$  implies that  $\chi_s^2 = {}^s\varepsilon/\varepsilon = 1$ . So  $\chi_{s,q}$ , the q-primary part of  $\chi_s$ , is the unique character of order 2 and conductor a power of q, that we denote by  $\xi_q$ . Since  $\xi_q$  has conductor q we see that  $v_q(\mathfrak{f}_L) = 1$ . For i = 0, 1 define  $G_q^i = \{\chi \in G \mid \chi_q = \xi_q^i\}$ . We have that  $G = G_q^0 \sqcup G_q^1$  and that the map  $\chi \mapsto \chi\chi_s$  is a bijection between  $G_q^0$  and  $G_q^1$ . Hence  $|G_q^0| = |G_q^1| = |G|/2$ . For  $\chi \in G_q^0$  we have that  $v_q(\mathfrak{f}_\chi) = 0$  and  $v_q(N_\chi) = v_q(N)$ . For  $\chi \in G_q^1$  we have that  $v_q(\mathfrak{f}_\chi) = 1 = v_q(\mathfrak{f}_L)$  and  $v_q(N_\chi) = v_q(N_\chi_s) = v_q(N)$ , because the level of  $f \otimes \chi_s$  is the level of  ${}^sf$  which is N. Plugging all this into (3) one obtains (4).

**Lemma 7.**  $\mathcal{N}_L(B)$  belongs to  $\mathbb{Z}$  if and only if  $[L : \mathbb{Q}]$  divides  $v_q(N_{L/\mathbb{Q}}(\mathcal{N}_L(B)))$  for all rational primes q.

Proof. Suppose that q decomposes in L as  $\mathfrak{q}_1^e \mathfrak{q}_2^e \cdots \mathfrak{q}_g^e$ . For each  $\sigma \in \operatorname{Gal}(L/\mathbb{Q})$  we have that  ${}^{\sigma}B$  is L-isogenous to B, so  $\mathcal{N}_L(B) = \mathcal{N}_L({}^{\sigma}B) = {}^{\sigma}\mathcal{N}_L(B)$ . This means that if  $\mathfrak{q}_1^n$  exactly divides  $\mathcal{N}_L(B)$  then the rest of  $\mathfrak{q}_i^n$  also exactly divide  $\mathcal{N}_L(B)$  and then  $v_q(N_{L/\mathbb{Q}}(\mathcal{N}_L(B))) = nfg$ , where f denotes the residual degree of  $\mathfrak{q}_i$ . Now  $\mathcal{N}_L(B)$  belongs to  $\mathbb{Z}$  if and only if for all primes q the exponent e divides n, and because of the relation  $efg = [L : \mathbb{Q}]$  this is equivalent to the fact that  $v_q(N_{L/\mathbb{Q}}(\mathcal{N}_L(B)))$  is divisible by  $[L : \mathbb{Q}]$ .

**Proposition 8.** If N is odd and  $\operatorname{ord}(\varepsilon) \leq 2$  then  $\mathcal{N}_L(B)$  belongs to  $\mathbb{Z}$  and  $\mathcal{N}_L(B) \,\mathfrak{f}_L^{\dim B} = N^{\dim B}.$ (5)

*Proof.* By lemma 6 for each prime q we have that  $v_q(N_{L/\mathbb{O}}(\mathcal{N}_L(B)))$  is multiple of  $[L:\mathbb{Q}]$ , and by lemma 7 this implies that  $\mathcal{N}_L(B)$  belongs to  $\mathbb{Z}$ . In consequence,  $N_{L/\mathbb{Q}}(\mathcal{N}_L(B)) = \mathcal{N}_L(B)^{[L:\mathbb{Q}]}$ , and using this in (4) we have that  $v_q(\mathcal{N}_L(B)) +$  $(\dim B) v_q(\mathfrak{f}_L) = (\dim B) v_q(N)$ . Since this holds for all q, the proposition follows.

Remark 9. If dim  $A_f = 2$  and  $\operatorname{ord}(\varepsilon) \leq 2$ , then either  $A_f$  is absolutely simple or it is isogenous over a quadratic number field L to the square of a  $\mathbb{Q}$ -curve B/L. In the second case it is always true that  $\mathcal{N}_L(B)$  belongs to  $\mathbb{Z}$  and  $\mathcal{N}_L(B)\mathfrak{f}_L = N$ . This follows by applying Milne's formula to the restriction of scalars of B, for which we have that  $\operatorname{Res}_{L/\mathbb{Q}}(B) \sim_{\mathbb{Q}} A_f$ .

Proposition 8 might be seen as a generalization of Carayol's formula  $\mathcal{N}_{\mathbb{Q}}(A_f) =$  $N^{\dim A_f}$  for modular abelian varieties. As we will see this formula does not generalize to arbitrary newforms; in other words, our hypothesis on the parity of Nand on the order of the character are necessary. However, for modular forms on  $\Gamma_0(N)$  and with arbitrary N it is still true except for a factor 2, that appears or not depending on the field L.

**Proposition 10.** Suppose that  $\varepsilon = 1$ . Then  $\mathcal{N}_L(B)$  is an integer and

(1) 2  $\mathcal{N}_L(B)$   $\mathfrak{f}_L^{\dim B} = N^{\dim B}$  if  $v_2(\mathfrak{f}_L) = 3$  and  $v_2(\mathfrak{f}_K) = 2$  for some  $K \subseteq L$ . (2)  $\mathcal{N}_L(B)$   $\mathfrak{f}_L^{\dim B} = N^{\dim B}$  otherwise.

In particular, if  $v_2(N) \leq 4$  the second formula holds.

*Proof.* Since  $\varepsilon$  is trivial the character  $\chi_s$  is quadratic for all  $s \in \text{Gal}(E/F)$ , so that any  $\chi \in G$  is quadratic. Define the set  $P_2 = \{\chi_2 \mid \chi \in G\}$ , which has cardinal  $\leq 4$ because the set of quadratic characters of conductor a power of 2 is isomorphic to  $\mathbb{Z}/2\mathbb{Z}\times\mathbb{Z}/2\mathbb{Z}$ . Observe that the condition  $v_2(\mathfrak{f}_L)=3$  and  $v_2(\mathfrak{f}_K)=2$  for some  $K \subseteq L$  is equivalent to  $|P_2| = 4$ . We begin by proving the second formula in the statement, which corresponds to the case  $|P_2| \leq 2$ .

If  $2 \nmid \mathfrak{f}_L$  then  $|P_2| = 1$  and

(6) 
$$v_2(N_{L/\mathbb{O}}(\mathcal{N}_L(B))) + [L:\mathbb{Q}] (\dim B) v_2(\mathfrak{f}_L) = [L:\mathbb{Q}] (\dim B) v_2(N).$$

If 2 |  $\mathfrak{f}_L$ , then for each  $s \in \operatorname{Gal}(E/F)$  the character  $\chi_{s,2}$  is either trivial or quadratic, so that the set  $P_2$  can have cardinal 2 or 4. Suppose first that  $|P_2| = 2$ , and fix an s such that  $\chi_{s,2} \in P_2$ . Then for i = 0, 1 define  $G_2^i = \{\chi \in G \mid \chi_2 = \chi_{s,2}^i\}$ . Observe that if  $\chi \in G_2^0$  then  $v_2(\mathfrak{f}_{\chi}) = 0$  and if  $\chi \in G_2^1$  then  $v_2(\mathfrak{f}_{\chi}) = v_2(\mathfrak{f}_L)$ . Moreover, for all  $\chi \in G$  we have that  $v_2(N_{\chi}) = v_2(N)$ , since  $v_2(N_{\chi}) = v_2(N_{\chi_s}) = v_2(N)$ . Now with the same reasoning as in lemma 6 we find that (6) also holds in this case. This, together with lemma 6 implies that the formula

(7) 
$$v_q(N_{L/\mathbb{Q}}(\mathcal{N}_L(B))) + [L:\mathbb{Q}] (\dim B) v_q(\mathfrak{f}_L) = [L:\mathbb{Q}] (\dim B) v_q(N)$$

is true for all q. Arguing as in the proof of proposition 8 this implies the second formula of the statement.

Suppose now that  $|P_2| = 4$ . If we denote by  $\xi$  and  $\psi$  the quadratic characters of conductor 8, then  $\xi\psi$  is the quadratic character of conductor 4 and  $P_2 = \{1, \xi, \psi, \xi\psi\}$ . Define  $G_{\xi} = \{\chi \in G \mid \chi_2 = \xi\}$ , and similarly for the other characters define  $G_{\psi}$ ,  $G_{\xi\psi}$  and  $G_1$ . Each one of these sets has cardinal |G|/4. If  $\chi$ 

belongs to  $G_{\xi}$  or  $G_{\psi}$ , then  $v_2(\mathfrak{f}_{\chi}) = 3$ , while if  $\chi$  belongs to  $G_{\chi\psi}$  then  $v_2(\mathfrak{f}_{\chi}) = 2$ . Therefore the relation (3) gives

$$v_2(N_{L/\mathbb{Q}}(\mathcal{N}_L(B))) + 2(\dim B)\left(2\frac{|G|}{4} + 3\frac{|G|}{4} + 3\frac{|G|}{4}\right) = |G|(\dim B)v_2(N),$$

and since now  $v_2(\mathfrak{f}_L) = 3$  we arrive at

 $v_2(N_{L/\mathbb{Q}}(\mathcal{N}_L(B))) + [L:\mathbb{Q}] (\dim B) (v_2(\mathfrak{f}_L) + 1) = [L:\mathbb{Q}] (\dim B) v_2(N).$ 

We see that in this case  $v_2(N_{L/\mathbb{Q}}(\mathcal{N}_L(B)))$  is also multiple of  $[L:\mathbb{Q}]$ . As before, for  $q \neq 2$  formula (7) also holds in this case, so we conclude that now  $2\mathcal{N}_L(B)\mathfrak{f}_L = N^{\dim B}$ .

To prove the last statement, let  $s \in \text{Gal}(E/F)$  and let  $\chi_s$  be the corresponding quadratic character. Then  $v_2(N_{\chi_s}) = v_2(N)$ , and if  $\varepsilon = 1$  and  $v_2(N) \leq 4$  by [1, Theorem 3.1] this is not possible if the conductor of  $\chi_{s,2}$  is 8. Therefore  $\chi_{s,2}$  is either trivial or the quadratic character of conductor 4, and we see that  $|P_2| \leq 2$ .

We remark that the first case in (10) does occur. For instance, let f be the unique (up to conjugation) normalized newform for  $\Gamma_0(512)$  such that  $A_f$  has dimension 4. Using Magma [4] one can compute the characters associated to the inner twists of f; it turns out that some of them have conductor divisible by 8 and some of them have conductor exactly divisible by 4 and therefore  $|P_2| = 4$ .

**Proposition 11.** If N is squarefree then for all primes q dividing N we have that

(1)  $v_q(N_{L/\mathbb{Q}}(\mathcal{N}_L(B))) = (\dim B)[L:\mathbb{Q}] \text{ if } q \nmid \mathfrak{f}_{\varepsilon}.$ 

(2)  $v_q(N_{L/\mathbb{Q}}(\mathcal{N}_L(B))) = 0 \text{ if } q \mid \mathfrak{f}_{\varepsilon}.$ 

In particular,  $\mathcal{N}_L(B)$  belongs to  $\mathbb{Z}$  and

(8) 
$$\mathcal{N}_L(B)\mathfrak{f}_L^{\dim B} = N^{\dim B}.$$

*Proof.* If  $q \nmid \mathfrak{f}_{\varepsilon}$  then  $v_q(\mathfrak{f}_{\chi}) = 0$  for all  $\chi \in G$  and then the formula follows easily from (3).

Suppose that  $q \mid \mathfrak{f}_{\varepsilon}$ . Let  $s \in \operatorname{Gal}(E/F)$  and let  $\chi_s$  be the character such that  ${}^sf = f \otimes \chi_s$ . Observe that  $v_q(N) = v_q(N_{\chi_s})$ , and by [1, Theorem 3.1] under our hypothesis this is possible if and only if  $\chi_{s,q} = 1$  or  $\chi_{s,q} = \varepsilon_q^{-1}$ . This means that for each  $\chi \in G$ , the character  $\chi_q$  is of the form  $\varepsilon_q^i$  for some *i*. In particular,  $v_q(\mathfrak{f}_L) = v_q(\mathfrak{f}_{\varepsilon})$ . Let  $n = \operatorname{ord}(\varepsilon_q)$ , and for  $i = 0, \ldots, n-1$  define  $G_q^i = \{\chi \in G \mid \chi_q = \varepsilon_q^i\}$ . The map  $\chi \mapsto \chi \varepsilon$  is a bijection between  $G_q^i$  and  $G_q^{i+1}$ , and since  $G = \bigsqcup_{i=0}^{n-1} G_q^i$  we see that  $|G_q^i| = |G|/n$ .

If  $\chi \in G_q^i$  then  $v_q(\mathfrak{f}_{\chi}) = 1$  for  $i = 1, \ldots, n-1$ , while  $v_q(\mathfrak{f}_{\chi}) = 0$  for i = 0. If  $\chi \in G_q^i$  for i = 0, n-1 then  $v_q(N_{\chi}) = v_q(N)$ ; if  $\chi \in G_q^0$  this is clear, and if  $\chi \in G_q^{n-1}$  this is because  $v_q(N_{\chi}) = v_q(N_{\varepsilon_q^{-1}}) = v_q(N_{\varepsilon^{-1}}) = v_q(N)$  since  $\overline{f} = f \otimes \varepsilon^{-1}$ . On the other hand, for the rest of the values  $i = 2, \ldots, n-2$  then  $v_q(N_{\chi}) = 2$  if  $\chi \in G_q^i$ ; this follows from [1, Theorem 3.1]. Gathering all this information we can rewrite 3 in this case as

$$v_q(N_{L/\mathbb{Q}}(\mathcal{N}_L(E))) + 2(\dim B) \sum_{i=0}^{n-1} \sum_{\chi \in G_q^i} v_q(\mathfrak{f}_\chi) = (\dim B) \sum_{i=0}^{n-1} \sum_{\chi \in G_q^i} v_q(N_\chi),$$

and this gives

$$v_q(N_{L/\mathbb{Q}}(\mathcal{N}_L(E))) + 2(\dim B) \frac{|G|}{n}(n-1) = (\dim B) \left( |G| + \frac{|G|}{n}(n-2) \right),$$

which is directly the formula for the second case.

Finally, the two formulas in the statement can be written as the following expression, which is valid for all q:

$$v_q(N_{L/\mathbb{Q}}(\mathcal{N}_L(B))) + [L:\mathbb{Q}] (\dim B) v_q(\mathfrak{f}_L) = [L:\mathbb{Q}] (\dim B) v_q(N).$$

This implies that  $\mathcal{N}_L(B)$  belongs to  $\mathbb{Z}$  and also the formula (8).

Remark 12. Observe that for squarefree N proposition 11 completely characterizes the places of good reduction of B: a prime  $\mathfrak{q} \mid q$  is a prime of good reduction of B if and only if  $q \nmid N$  or  $q \mid \mathfrak{f}_{\varepsilon}$ .

## 4. Examples

In this section we show explicit examples of building blocks of dimension one and two where we compute their conductors. As in the rest of the paper, all the newforms we consider are without complex multiplication.

4.1. Q-curves. All the examples in this paragraph come from modular abelian varieties  $A_f$  where the corresponding building block B has dimension one. An algorithm to compute equations of building blocks of dimension one is provided by González and Lario in [8]. The equations for the first three examples were computed using that algorithm, and the equations for examples 14 and 15 have been provided by Jordi Quer. The conductor of these elliptic curves have been computed using Magma.

**Example 13.** Let f be the unique (up to conjugation) normalized newform of weight two, level 42 and Nebentypus of order 2 and conductor 21. We have dim  $A_f = 4$  and  $L = \mathbb{Q}(\sqrt{-3}, \sqrt{-7})$ . In [8] it is proved that an equation for B is given by

$$B: y^2 = x^3 + \frac{81}{4}(69 + 43\sqrt{-3} + 29\sqrt{-7} + 17\sqrt{21})x + 162(207 - 84\sqrt{-3} - 54\sqrt{-7} + 46\sqrt{21})$$

We have  $\mathcal{N}_L(B) = 2$  and  $\mathfrak{f}_L = 21$ . Therefore we have that the Proposition 8 holds although N is even in this case.

**Example 14.** Let f be the unique (up to conjugation) normalized newform of weight two, level 64 and Nebentypus of order 4 and conductor 16. In this case,  $A_f$  is an abelian surface and  $L = \mathbb{Q}(\alpha)$ , where  $\alpha^4 - 4\alpha^2 + 2 = 0$ . An equation for B is

$$B: y^2 = x^3 - 432(5 - 8\alpha + 14\alpha^2 - 6\alpha^3)x - 864(-124 + 74\alpha + 194\alpha^2 - 107\alpha^3).$$

We have  $\mathcal{N}_L(B) = 2$  and  $\mathfrak{f}_L = 16$ . Therefore we have that  $2 \mathcal{N}_L(B) \mathfrak{f}_L^{\dim B} = N^{\dim B}$ .

**Example 15.** Let f be the unique (up to conjugation) normalized newform (without complex multiplication) of weight two, level 81 and Nebentypus of order 3 and conductor 9. In this case, dim  $A_f = 4$  and  $L = \mathbb{Q}(\sqrt{-3}, \alpha)$ , where  $\alpha^3 - 3\alpha + 1 = 0$ . An equation for the building block is:

$$B: y^2 = x^3 - \frac{81}{2}(-54 + 14\sqrt{-3} + 2(12 + 5\sqrt{-3})\alpha + (27 - 7\sqrt{-3})\alpha^2)x + 729(37 + 19\sqrt{-3}).$$

We have  $\mathcal{N}_L(B) = 3$  and  $\mathfrak{f}_L = 9$ . Therefore we have that  $3 \mathcal{N}_L(B) \mathfrak{f}_L^{\dim B} = N^{\dim B}$ .

In the above examples the conductors  $\mathcal{N}_L(B)$  turned out to be rational integers. The following example shows that this is not always the case. **Example 16.** There are two normalized newforms of weight two, level 98 and Nebentypus  $\varepsilon$  of order 3 and conductor 7 such that the the associated abelian variety is a surface. In both cases  $L = \mathbb{Q}(\alpha)$ , where  $\alpha^3 + \alpha^2 - 2\alpha - 1 = 0$ . To obtain an equation for the building block we are going to proceed in a different way than above. Let f be one of these two newforms. Then,  $A_f \sim_L B^2$  and by Proposition 4 we have that  $\operatorname{Res}_{L/\mathbb{Q}}(B) \sim_{\mathbb{Q}} A_f \times A_{f\otimes\varepsilon}$ . Therefore  $\dim A_{f\otimes\varepsilon} = 1$ . In particular,  $B \sim_L A_{f\otimes\varepsilon}$ . Then, instead of computing an equation of B/L using the González-Lario algorithm [8] we are going to compute an equation of  $A_{f\otimes\varepsilon}$  over  $\mathbb{Q}$ . In this case the results of Atkin and Li [1] do not provide the exact level of  $f \otimes \varepsilon$ , althought they assert that the level is a divisor of 98 of the form  $2 \cdot 7^n$ . One of the twisted newforms corresponds to the unique (up to  $\mathbb{Q}$ -isogeny) elliptic curve defined over  $\mathbb{Q}$  of level 14 and the other one to the unique (up to  $\mathbb{Q}$ -isogeny) elliptic curve defined over  $\mathbb{Q}$  of level 98 (they are labelled as 14A and 98A respectively in Cremona's tables [6] or in Antwerp tables [2]). The equations for these building blocks are:

$$B_1 : y^2 + xy + y = x^3 + 4x - 6, B_2 : y^2 + xy = x^3 + x^2 - 25x - 111$$

For i = 1, 2, we have  $\mathcal{N}_L(B_i) = 2(\alpha^2 - \alpha - 2)^i \cdot \mathcal{O}_L$ , which is not an ideal generated by a rational integer.

4.2. **Genus** 2 **curves.** In the opposite to the elliptic curve case, there is no implementation of an algorithm to compute the conductor of a genus 2 curve over a number field. For that purpose, Proposition 5 allows us to compute the conductor of a genus 2 curve that corresponds to the building block of a modular abelian variety.

**Example 17.** Let *C* be the genus 2 curve defined over  $\mathbb{Q}(\sqrt{-6})$  defined by  $C: y^2 = (27\sqrt{-6} - 324)x^6 - 15876x^5 + (-7938\sqrt{-6} - 222264)x^4 - 345744x^3 + (-259308\sqrt{-6} + 7260624)x^2 - 16941456x + 941192\sqrt{-6} + 11294304.$ 

The jacobian  $B = \operatorname{Jac}(C)$  is a building block with quaternionic multiplication, and in [7] it is proved that  $\operatorname{Res}_{L/\mathbb{Q}}(B)$  is isogenous to a product of modular abelian varieties over  $\mathbb{Q}$ , where  $L = \mathbb{Q}(\sqrt{2}, \sqrt{-3})$ . In fact, there are numerical evidences suggesting that  $\operatorname{Res}_{L/\mathbb{Q}}(B) \sim_{\mathbb{Q}} A_f^2$ , where f is a newform of level  $N = 2^{8}3^5$  and Nebentypus  $\varepsilon$  of order 2 and conductor 8 with dim  $A_f = 4$ . Assuming this we are going to prove that  $\mathcal{N}_L(B) = 2^{10}3^8$ , and therefore the formula  $\mathcal{N}_L(B) \mathfrak{f}_L^{\dim B} = N^{\dim B}$ would hold again. The subfields of L are the quadratic fields  $\mathbb{Q}(\sqrt{2})$ ,  $\mathbb{Q}(\sqrt{-3})$  and  $\mathbb{Q}(\sqrt{-6})$ , and they correspond to the non-trivial homomorphisms from G to  $\mathbb{C}^{\times}$ . Therefore the conductors of these quadratic fields correspond to the conductors of the non-trivial elements at G. On the other hand, by the decomposition of  $\operatorname{Res}_{L/\mathbb{Q}}(B)$  given above and by [1, Theorem 3.1] we have that  $N_{\chi} = N$  for all  $\chi \in G$ . Now, Proposition 5 at the primes q = 2 and q = 3 give us the stated conductor of B over L.

Acknowledgements. We thank A. Brumer for useful discussion on conductors of abelian varieties and J. Quer for providing us equations for some of the examples of Section 4.

#### References

 A.O.L Atkin, W.C.W. Li, Twists of Newforms and Pseudo-Eigenvalues of W-operators. Invent. Math. 48 (1978), no. 3, 221–243.

- [2] B. J. Birch; W. Kuyk (eds.), Modular Functions of One Variable IV. Lecture Notes in Mathematics 476, Springer-Verlag, 1975.
- [3] C. Breuil, B. Conrad, F. Diamond, and R. Taylor, On the modularity of elliptic curves over Q: wild 3-adic exercises. J. Amer. Math. Soc., 14(4):843–939, 2001.
- [4] J. J. Cannon, W. Bosma (Eds.), Handbook of Magma Functions, Edition 2.15-13 (2009).
- [5] H. Carayol, Sur les reprèsentations galoisiennes modulo l attachées aux formes modulaires. Duke Math. J. 59 (1989), no. 3, 785–801.
- [6] J. E. Cremona, Algorithms for modular elliptic curves, Cambridge University Press 1992.
- [7] X. Guitart, J. Quer, Modular abelian varieties over number fields. Submitted. arXiv:0905.2550.
- [8] J. González, J-C. Lario, Q-curves and their Manin ideals. Amer. J. Math. 123 (2001), no. 3, 475–503.
- [9] J. S. Milne, On the arithmetic of abelian varieties. Invent. Math. 17 (1972), 177-190.
- [10] E. E. Pyle. Abelian varieties over Q with large endomorphism algebras and their simple components over Q. Modular curves and abelian varieties, Progress in Math., vol. 224 (2002), pp. 189–239.
- [11] K. Ribet, Twists of modular forms and endomorphisms of abelian varieties. Math. Ann. 253 (1980), no. 1, 43–62.
- [12] K. Ribet, Abelian varieties over Q and modular forms. Algebra and topology 1992 (Taejŏn), 53–79, Korea Adv. Inst. Sci. Tech., Taejŏn, 1992. Reprinted on Modular curves and abelian varieties, 241–261, Progr. Math. 224, Birkhäuser, Basel, 2004.
- [13] G. Shimura. On the factors of the jacobian variety of a modular function field. J. Math. Soc. Japan, 25(3), 523–544, 1973.
- [14] Washington, Introduction to cyclotomic fields. Second edition. GTM, 83. Springer-Verlag, New York, 1997.
- [15] A. Wiles, Modular elliptic curves and Fermat's last theorem. Ann. of Math. (2), 141(3):443– 551, 1995.

UNIVERSIDAD AUTÓNOMA DE MADRID, DEPARTAMENTO DE MATEMÁTICAS AND INSTITUTO DE CIENCIAS MATEMÁTICAS (CSIC-UAM-UC3M-UCM), MADRID, SPAIN E-mail address: enrique.gonzalez.jimenez@uam.es

Departament de Matemàtica aplicada II, Universitat Politècnica de Catalunya, Jordi Girona 1-3 (Edifici Omega) 08034, Barcelona

*E-mail address*: xevi.guitart@gmail.com