

# ON THE EQUATION $a^2 + b^{2p} = c^5$

IMIN CHEN

ABSTRACT. Using the method of Galois representations and modular forms, we show that the generalized Fermat equation  $a^2 + b^{2p} = c^5$  does not have any non-trivial proper solutions if  $p > 17$  is a prime such that  $p \equiv 1 \pmod{4}$ . In order to apply the method, we use  $\mathbb{Q}$ -curves defined over quartic extensions of  $\mathbb{Q}$  and consider the abelian varieties of  $\mathrm{GL}_2$ -type attached to them.

A solution  $(a, b, c) \in \mathbb{Z}^3$  to the equation  $a^2 + b^{2p} = c^5$  is said to be non-trivial if  $ab \neq 0$  and proper if  $(a, b, c) = 1$ . This equation is a special case of the generalized Fermat equation  $x^p + y^q = z^r$  which has been the focus of much interest since the resolution of Fermat's Last Theorem (cf. [20] and its references for a survey of recent work in this area).

In this paper, we show the following result.

**Theorem 1.** *Let  $p > 17$  be a prime such that  $p \equiv 1 \pmod{4}$ . Then the equation  $a^2 + b^{2p} = c^5$  does not have any non-trivial proper solutions.*

The method uses Galois representations and modular forms. A new feature which arises for this equation is the use of  $\mathbb{Q}$ -curves defined over quartic extensions of  $\mathbb{Q}$  and the abelian varieties of  $\mathrm{GL}_2$ -type attached to them. To handle the  $\mathbb{Q}$ -curves in the method, we use the results developed in [14], where the use of  $\mathbb{Q}$ -curves was first introduced. However, to deal with  $\mathbb{Q}$ -curves defined over quartic extensions of  $\mathbb{Q}$ , it is necessary to use some results from the theory of  $\mathbb{Q}$ -curves [17] [30] [27] [15] and make them sufficiently explicit.

Finally, we note the overall strategy still cannot handle certain primes  $p$  due to our inability to apply Mazur's method to analyze the rational points

---

*Date:* 1 August 2007.

*2000 Mathematics Subject Classification.* Primary: 11D41, Secondary: 11G05, 11D61, 14G05.

*Key words and phrases.* Generalized Fermat equations,  $\mathbb{Q}$ -curves, Galois representations, modular forms, elliptic curves over number fields.

Research supported by NSERC.

on certain modular curves with non-split Cartan level structure (cf. Remark 3.7 in [14]). This happens because the sign of the functional equation for the  $L$ -function of the jacobian of the modular curve  $X_{0,N'}^K(d,p)$  (see paragraph after Theorem 45) for  $d = 2$  and  $K = \mathbb{Q}(\sqrt{5})$  is  $-1$ , using [2] for instance, so conjecturally that these jacobians do not have any non-zero quotients over  $\mathbb{Q}$  with rank 0 (see Section 6). The situation still doesn't change if the  $N'$  level structure on mod  $p$  torsion points is replaced by a twisted  $C'$  level structure.

### 1. SETTING UP THE PROBLEM

We begin by recalling the parametrization of proper solutions to the equation  $x^2 + y^2 = z^5$ .

**Lemma 2.** *A triple  $(x, y, z) \in \mathbb{Z}^3$  with  $(x, y, z) = 1$  satisfies  $x^2 + y^2 = z^5$  only if  $(x, y, z) = (u(u^4 - 10u^2v^2 + 5v^4), v(v^4 - 10v^2u^2 + 5u^4), u^2 + v^2)$  for some  $(u, v) \in \mathbb{Z}^2$  with  $(u, v) = 1$ .*

*Proof.* This follows from factoring over the Gaussian integers.  $\square$

**Lemma 3.** *Let  $p$  be an odd prime. Suppose  $(a, b, c) \in \mathbb{Z}^3$  satisfies  $a^2 + b^{2p} = c^5$  with  $(a, b, c) = 1$  and  $ab \neq 0$ . Then there exists  $(s, t) \in \mathbb{Z}^2$  with  $(s, t) = 1$ ,  $st \neq 0$ , and such that the following properties hold:*

- $s^2 - 10st + 5t^2 = 5^j \gamma^p$  where  $5 \nmid \gamma$
- $v = \beta^p$  and  $j = 0$  or  $v = 5^{kp-1} \beta^p$  and  $j = 1$ , where  $5 \nmid \beta$  and  $k \geq 1$
- $s = v^2, t = u^2$ .

*Proof.* As  $(u, v) = 1$ , we have that  $(v, v^4 - 10v^2u^2 + 5u^4) \mid 5$ . Setting  $y$  to be a  $p$ -th power in Lemma 2, we obtain a solution to

$$v^4 - 10v^2u^2 + 5u^4 = 5^j \gamma^p$$

where  $(u, v) = 1$ ,  $uv \neq 0$ ,  $5 \nmid \gamma$  and  $j \geq 0$ . Setting  $s = v^2$ ,  $t = u^2$  we have that

$$s^2 - 10st + 5t^2 = 5^j \gamma^p.$$

Since in fact  $(v^2, v^4 - 10v^2u^2 + 5u^4) \mid 5$ , we either have  $5 \nmid s$  and  $j = 0$  or  $5 \mid s$  and  $j = 1$ . Thus, we either have  $v = \beta^p$  and  $j = 0$  or  $v = 5^{kp-1} \beta^p$  and  $j = 1$ , where  $5 \nmid \beta$  and  $k \geq 1$ .  $\square$

For the equation  $a^{2p} + b^{2p} = c^5$ , one can set both  $x$  and  $y$  to be a  $p$ -th power and consider the resulting diophantine equations. Bennett [3] has shown these equations can be resolved using the results in [4].

It is perhaps instructive to discuss in more detail how the argument proceeds. If we use the constraint that  $y$  is a  $p$ -th power, we can complete the square in the following way to obtain a solution to an equation of the form  $Aa'^m + Bb'^n = Cc'^2$ ,

$$\begin{aligned} v^4 - 10v^2u^2 + 5u^4 &= 5(u^2 - v^2)^2 - 4v^4 \\ &= \begin{cases} 5(u^2 - v^2)^2 - 4\beta^{4p} = \gamma^p & \text{if } j = 0 \\ 5(u^2 - v^2)^2 - 4 \cdot 5^{4kp-4}\beta^{4p} = 5\gamma^p & \text{if } j = 1. \end{cases} \end{aligned}$$

In [4], this class of generalized Fermat equations was extensively studied from the point of view of the modular method. The elliptic curve which they attach to a solution  $(a', b', c')$  is isomorphic over  $\mathbb{Q}$  to  $Y^2 = X^3 + 2c'CX^2 + BCb'^nX$ , and has the preconditions required to be a candidate Frey curve for solving the constraints that  $v, s^2 - 10st + 5t^2$  are  $p$ -powers up to  $S$ -units for a finite set of primes  $S$ , using the modular method.

Unfortunately, in the case of  $j = 0$ , the solution corresponding to  $(u, v) = (0, 1)$  persists for all  $p$  and the Frey curve [4] corresponding to this solution does not have complex multiplication. This is a situation for which one is not currently able to apply the modular method to obtain a full result in every congruence class. In the case of  $j = 1$ , that is, when  $5 \mid y$ , there is an obstructing newform in  $S_2(\Gamma_0(40))$  which prevents a resolution in the situation when  $a'b'$  is odd.

Some partial results are possible however. For instance, one can give a computational criterion for resolving specific primes  $p$  when  $5 \mid y$ , using the technique of [19] (cf. also [9]). Also, one has a resolution for  $p \geq 7$  and  $y$  even using the results in [4]. Because of the symmetry between  $a$  and  $b$  in the equation  $a^{2p} + b^{2p} = c^5$ , we may assume  $y$  is even, hence Bennett's result [3].

**Lemma 4.** *Let  $p$  be an odd prime. If  $s^2 - 10st + 5t^2 = 5^j\gamma^p$  where  $j \in \{0, 1\}$ ,  $5 \nmid \gamma$ , and  $s, t \in \mathbb{Z}$  are coprime squares, then  $s \not\equiv t \pmod{2}$  and  $s^2 - 10st + 5t^2$  is not divisible by 2.*

*Proof.* If  $s \equiv t \pmod{2}$ , then  $s \equiv t \pmod{8}$  and  $s, t \not\equiv 0 \pmod{2}$  as  $s, t$  are coprime squares. Then we would have that  $5^j \gamma^p = s^2 - 10st + 5t^2 \equiv -4s^2 \pmod{8}$ . This is a contradiction if  $p$  is an odd prime.  $\square$

**Lemma 5.** *Let  $p$  be an odd prime. If  $s^2 - 10st + 5t^2 = 5^j \gamma^p$  where  $j \in \{0, 1\}$ ,  $5 \nmid \gamma$ , and  $s, t \in \mathbb{Z}$  are coprime squares, then  $s^2 - 10st + 5t^2$  is not divisible by 3.*

*Proof.* We note that  $s^2 - 10st + 5t^2 \equiv s^2 - st - t^2 \pmod{3}$  is irreducible when considered as an element of  $\mathbb{F}_3[s, t]$ .  $\square$

For the next two lemmas, we note that  $v^4 - 10v^2t + 5t^2 = 5(t - v^2)^2 - 4v^4$  so integer solutions to  $v^4 - 10v^2t + 5t^2 = c$  give rise to integer solutions to  $5Y^2 - 4X^4 = c$ .

**Lemma 6.** *If  $(v, t) \in \mathbb{Z}^2$  satisfies  $v^4 - 10v^2t + 5t^2 = \pm 1$ , then  $v = \pm 1$  and  $t = 0$ .*

*Proof.* We use the Elliptic Curves package in MAGMA [5] to determine the integer solutions to the quartic equation  $5Y^2 = 4X^4 \pm 1$ .  $\square$

**Lemma 7.** *If  $(v, t) \in \mathbb{Z}^2$  satisfies  $v^4 - 10v^2t + 5t^2 = \pm 5$ , then  $v = 0$  and  $t = \pm 1$ .*

*Proof.* We use the Elliptic Curves package in MAGMA [5] to determine the integer solutions to the quartic equation  $5Y^2 = 4X^4 \pm 5$ .  $\square$

**Corollary 8.** *Let  $p$  be an odd prime. Suppose  $(a, b, c) \in \mathbb{Z}^3$  satisfies  $a^2 + b^{2p} = c^5$  with  $(a, b, c) = 1$  and  $ab \neq 0$ . Let  $s, t$  be as in Lemma 3. Then  $s^2 - 10st + 5t^2$  is divisible by a prime not equal to 2, 3, 5.*

*Proof.* By Lemmas 3, 4, and 5, we see that if  $s^2 - 10st + 5t^2$  is only divisible by the primes 2, 3, 5, then  $s^2 - 10st + 5t^2 = \pm 1, \pm 5$ . The result then follows from Lemmas 6 and 7.  $\square$

## 2. $\mathbb{Q}$ -CURVES AND ABELIAN VARIETIES OF $\mathrm{GL}_2$ -TYPE

Let  $K$  be a number field and let  $C$  be an elliptic curve defined over  $K$  such that there is an isogeny  $\mu_C(\sigma) : {}^\sigma C \rightarrow C$  defined over  $K$  for each  $\sigma \in G_{\mathbb{Q}}$ . Such an elliptic curve  $C$  is called a  $\mathbb{Q}$ -curve defined over  $K$ . This

notion was originally defined and studied for a CM-elliptic curve [17] [6], but was extended by Ribet [30] to the non-CM case using different methods. Further explicit considerations were developed in [27] which we will use in the sequel. The exposition below of the theory follows closely the citations above as well as [15].

From here on, we choose the isogenies so that  $\mu_C(\sigma)$  factors through  $G_{K/\mathbb{Q}}$  and  $\mu_C(\sigma)$  is the identity on  $G_K$ . Furthermore, when we speak of a  $\mathbb{Q}$ -curve, we will assume that it does not have complex multiplication.

Let  $c_C(\sigma, \tau) = \mu_C(\sigma)^\sigma \mu_C(\tau) \mu_C(\sigma\tau)^{-1} \in (\text{Hom}_K(C, C) \otimes_{\mathbb{Z}} \mathbb{Q})^* = \mathbb{Q}^*$ , where  $\mu_C^{-1} := (1/\deg \mu_C) \mu'_C$  and  $\mu'_C$  is the dual of  $\mu_C$ . Then  $c_C(\sigma, \tau)$  determines a class in  $H^2(G_{\mathbb{Q}}, \mathbb{Q}^*)$  which depends only on the  $\overline{\mathbb{Q}}$ -isogeny class of  $C$ . The class  $c_C(\sigma, \tau)$  factors through  $H^2(G_{K/\mathbb{Q}}, \mathbb{Q}^*)$  and this class depends only on the  $K$ -isogeny class of  $C$ . Moreover,  $c_C(\sigma, \tau)$  in fact lies in  $H^2(G_{\mathbb{Q}}, \mathbb{Q}^*)[2]$ .

Tate (cf. [32, Theorem 4]) showed that  $H^2(G_{\mathbb{Q}}, \overline{\mathbb{Q}}^*)$  is trivial where the action of  $G_{\mathbb{Q}}$  on  $\overline{\mathbb{Q}}^*$  is trivial. Thus, there is a continuous map  $\beta : G_{\mathbb{Q}} \rightarrow \overline{\mathbb{Q}}^*$  such that

$$c_C(\sigma, \tau) = \beta(\sigma)\beta(\tau)\beta(\sigma\tau)^{-1}$$

as cocycles in  $H^2(G_{\mathbb{Q}}, \overline{\mathbb{Q}}^*)$ . In such a case, we say that  $\beta$  is a splitting map for  $C$  (or more precisely, for  $c_C(\sigma, \tau)$ ).

Let  $A$  be an abelian variety defined over  $\mathbb{Q}$ . The endomorphism algebra  $\text{End}_{\mathbb{Q}} A$  of  $A$  is defined as the ring of endomorphisms of  $A$  defined over  $\mathbb{Q}$  tensored over  $\mathbb{Z}$  with  $\mathbb{Q}$ . Let  $\mathcal{R}_C$  be the  $\mathbb{Q}$ -algebra generated over  $\mathbb{Q}$  by  $\lambda_\sigma$  for  $\sigma \in G_{K/\mathbb{Q}}$  with multiplication given by  $\lambda_{\sigma\tau} c_C(\sigma, \tau) = \lambda_\sigma \lambda_\tau$ , where we recall that  $c_C(\sigma, \tau) = \mu_C(\sigma)^\sigma \mu_C(\tau) \mu_C(\sigma\tau)^{-1}$  depends the function  $\mu_C$ . Consider the restriction of scalars  $\text{Res}_{\mathbb{Q}}^K C$ , for which we recall its defining functorial property that  $\text{Hom}(S, \text{Res}_{\mathbb{Q}}^K C) \leftrightarrow \text{Hom}(S \otimes K, C)$ . There is a natural isomorphism

$$\mathcal{R}_C \rightarrow \text{End}_{\mathbb{Q}} \text{Res}_{\mathbb{Q}}^K C$$

which sends  $\lambda_\sigma$  to the endomorphism of  $\text{Res}_{\mathbb{Q}}^K C$  defined by

$$P \mapsto {}^\tau \mu_C(\sigma)(P)$$

on  ${}^{\sigma\tau} C$ .

Given a splitting map  $\beta$  for  $C$ , we now enlarge  $K$  if necessary so that  $\beta$  factors through  $G_{K/\mathbb{Q}}$ . The map given by  $\lambda_\sigma \mapsto \beta(\sigma)$  gives a surjective homomorphism  $\mathcal{R}_C \rightarrow M_\beta = \mathbb{Q}(\beta(\sigma))$ . As  $\mathcal{R}_C$  is a semi-simple  $\mathbb{Q}$ -algebra, there is a projection from  $\mathcal{R}_C$  onto the isomorphic copy of  $M_\beta$  in  $\mathcal{R}_C$ . Let  $A_\beta$  be the image of this projection in the category of abelian varieties defined over  $\mathbb{Q}$  up to isogeny over  $\mathbb{Q}$ .

We note the following twist on the construction of  $A_\beta$  above which is useful in practice to minimize the degree of the extension  $K$  required (recall  $K$  needs to be large enough so both  $c_C(\sigma, \tau)$  and  $\beta(\sigma)$  factor through  $G_{K/\mathbb{Q}}$ ). Suppose that as 2-cocycles we have that

$$c_C(\sigma, \tau)\epsilon(\sigma, \tau) = \beta(\sigma)\beta(\tau)\beta(\sigma\tau)^{-1}$$

where  $\epsilon(\sigma, \tau)$  is the 2-coboundary obtained from a 1-cocycle  $\frac{\sigma\sqrt{\gamma}}{\sqrt{\gamma}}$  where  $\gamma \in \overline{\mathbb{Q}}^*$ . By the way twisting affects the cocycles  $c_C(\sigma, \tau)$  [27, p. 291] we see that the twist  $C_\gamma$  of  $C$  is such that

$$c_{C_\gamma}(\sigma, \tau) = c_C(\sigma, \tau)\epsilon(\sigma, \tau) = \beta(\sigma)\beta(\tau)\beta(\sigma\tau)^{-1}.$$

Thus, replacing  $C$  by  $C_\gamma$  allows us to only require that  $K$  be large enough so that  $\beta(\sigma)$  factors through  $G_{K/\mathbb{Q}}$ .

Recall an abelian variety defined over  $\mathbb{Q}$  of  $\mathrm{GL}_2$ -type is one whose endomorphism algebra is isomorphic to a number field  $M$  of degree equal to the dimension of the abelian variety. An abelian variety defined over  $\mathbb{Q}$  of  $\mathrm{GL}_2$ -type attached to a  $\mathbb{Q}$ -curve  $C$  is one which has  $C$  as a quotient over  $\overline{\mathbb{Q}}$ .

**Theorem 9.** *The abelian variety  $A_\beta$  is an abelian variety defined over  $\mathbb{Q}$  of  $\mathrm{GL}_2$ -type attached to  $C$ , with endomorphism algebra isomorphic to  $M_\beta$ .*

*Proof.* cf. [30, Theorem 6.1]. □

**Proposition 10.** *If  $A$  is an abelian variety defined over  $\mathbb{Q}$  of  $\mathrm{GL}_2$ -type attached to a  $\mathbb{Q}$ -curve  $C$ , then  $A$  is isogenous over  $\mathbb{Q}$  to some  $A_\beta$  where  $\beta$  is a splitting map for  $C$ .*

*Proof.* If  $C$  is a quotient of  $A$  defined over  $K$ , then there is a non-zero homomorphism  $A \rightarrow \mathrm{Res}_{\mathbb{Q}}^K C$  defined over  $\mathbb{Q}$ . Since  $A$  is simple up to isogeny over  $\mathbb{Q}$ , it follows that  $A$  is a quotient defined over  $\mathbb{Q}$  of  $\mathrm{Res}_{\mathbb{Q}}^K C$ . As  $\mathcal{R}_C$  is a semi-simple  $\mathbb{Q}$ -algebra, there is a projection  $\mathcal{R}_C \rightarrow \mathrm{End}_{\mathbb{Q}} A$  given

by  $\lambda_\sigma \rightarrow \beta(\sigma)$  say. We now see that  $\beta$  is a splitting map for  $C$ , and that  $A_\beta$  is isogenous over  $\mathbb{Q}$  to  $A$ .  $\square$

**Proposition 11.** *Suppose that  $\mathcal{R}_C$  is a product of fields. Then  $\text{Res}_{\mathbb{Q}}^K C$  is isogenous over  $\mathbb{Q}$  to a product of pairwise non-isogenous abelian varieties defined over  $\mathbb{Q}$  of  $\text{GL}_2$ -type, each of the form  $A_\beta$  where  $\beta$  is a splitting map for  $C$ . Furthermore,  $A_{\beta_1}$  is isogenous over  $\mathbb{Q}$  to  $A_{\beta_2}$  if and only if  $\beta_2 = {}^\sigma\beta_1$  for some  $\sigma \in G_{\mathbb{Q}}$ .*

*Proof.* cf. [27, Proposition 5.1, Lemma 5.3].  $\square$

For an abelian variety  $A$  defined over  $\mathbb{Q}$ , let  $\hat{V}_p(C)$  denote the  $\mathbb{Q}_p[G_{\mathbb{Q}}]$ -module which is the  $p$ -adic Tate module of  $C$  tensored over  $\mathbb{Q}_p$ .

**Proposition 12.**  $\hat{V}_p(\text{Res}_{\mathbb{Q}}^K C) \cong \mathcal{R}_C \otimes \hat{V}_p(C)$  as  $\mathcal{R}_C \otimes \mathbb{Q}_p[G_{\mathbb{Q}}]$ -modules.

*Proof.* The proof is a modification of [30, Corollary 6.6]. Recall that it is given that  $C$  is a  $\mathbb{Q}$ -curve defined over  $K$  and let  $A = \text{Res}_{\mathbb{Q}}^K C$ . There is an isomorphism  $A \cong B_K = \prod_{\sigma \in G_{K/\mathbb{Q}}} {}^\sigma C$  defined over  $K$  by the defining property of restriction of scalars. Let  $T_K = \prod_{\sigma \in G_{K/\mathbb{Q}}} C_\sigma$  where  $C_\sigma = C$  for all  $\sigma \in G_{K/\mathbb{Q}}$ . There is an action of  $\mathcal{R}_C$  on  $T_K$  with  $\lambda_g$  taking the factor  $C_\sigma$  to the factor  $C_{g\sigma}$  via multiplication by  $c_C(g, \sigma)$ . Let  $\iota : T_K \rightarrow B_K$  be the map which takes the factor  $C_\sigma$  to the factor  ${}^{\sigma^{-1}}C$  via the map  ${}^{\sigma^{-1}}\mu_C(\sigma)$ . Then  $\iota$  is a  $\mathcal{R}_C[G_K]$ -equivariant isomorphism. By the defined action of  $\mathcal{R}_C$  on  $T_K$ , we have that  $\hat{V}_p(T_K) \cong \mathcal{R}_C \otimes \hat{V}_p(C)$  as  $\mathcal{R}_C \otimes \mathbb{Q}_p[G_K]$ -modules. Hence,  $\hat{V}_p(A) \cong \hat{V}_p(B_K) \cong \mathcal{R}_C \otimes \hat{V}_p(C)$  as  $\mathcal{R}_C \otimes \mathbb{Q}_p[G_K]$ -modules. The action of  $G_{\mathbb{Q}}$  on  $A$  can be transferred to an action of  $G_{\mathbb{Q}}$  on  $T_K$  via the isomorphisms  $A \cong B_K \cong T_K$ . From this, it can be shown that the explicit action of  $G_{\mathbb{Q}}$  on the  $\mathcal{R}_C \otimes \mathbb{Q}_p$ -module  $\hat{V}_p(A) \cong \mathcal{R}_C \otimes \hat{V}_p(C)$  is given by

$$x \otimes y \mapsto x \cdot \lambda_{\sigma^{-1}} \otimes ({}^\tau\mu_C(\tau^{-1}))^{-1}(\tau(y)).$$

$\square$

From Proposition 12, it follows that  $\hat{V}_p(A_\beta) \cong M_\beta \otimes \hat{V}_p(C)$  as  $M_\beta \otimes \mathbb{Q}_p[G_{\mathbb{Q}}]$ -modules. Picking a prime  $\pi$  of  $M_\beta$  above  $p$ , we get a representation  $\hat{\rho}_{C, \beta, \pi} : G_{\mathbb{Q}} \rightarrow \text{GL}_2(M_{\beta, \pi})$ . The explicit action of  $G_{\mathbb{Q}}$  on the  $M_\beta \otimes \mathbb{Q}_p$  module  $\hat{V}_p(A_\beta)$  is then given by

$$x \otimes y \mapsto x \cdot \beta(\sigma^{-1}) \otimes ({}^\tau\mu_C(\tau^{-1}))^{-1}(\tau(y)),$$

which can be simplified to the expression

$$x \otimes y \mapsto x \cdot \beta(\sigma)^{-1} \otimes \mu_C(\tau)(\tau(y)).$$

Hence, if we regard  $M_{\beta,\pi}$  as a subfield of  $\overline{\mathbb{Q}}_p$ , then  $\hat{\rho}_{C,\beta,\pi}$  is a representation to  $\overline{\mathbb{Q}}_p^* \cdot \mathrm{GL}_2(\mathbb{Q}_p)$ , and it satisfies  $\mathbb{P}\hat{\rho}_{C,\beta,\pi}|_{G_K} \cong \mathbb{P}\hat{\phi}_{C,p}$ , where  $\hat{\phi}_{C,p} : G_K \rightarrow \mathrm{GL}_2(\mathbb{Q}_p)$  is the representation of  $G_K$  on  $\hat{V}_p(C)$ .

Let  $\epsilon_\beta : G_{\mathbb{Q}} \rightarrow \overline{\mathbb{Q}}^*$  be defined by

$$\epsilon_\beta(\sigma) = \beta(\sigma)^2 / \deg \mu_C(\sigma).$$

Then  $\epsilon_\beta$  is a character and

$$(1) \quad \det \hat{\rho}_{C,\beta,\pi} = \epsilon_\beta^{-1} \cdot \chi_p,$$

where  $\chi_p : G_{\mathbb{Q}} \rightarrow \mathbb{Z}_p^*$  is the  $p$ -th cyclotomic character.

Given two splitting maps  $\beta, \beta'$  for  $C$ , there is a character  $\chi : G_{\mathbb{Q}} \rightarrow \overline{\mathbb{Q}}^*$  such that  $\beta' = \chi\beta$ . Conversely, if  $\beta$  is a splitting map, then  $\beta' = \chi\beta$  is a splitting map for any character  $\chi : G_{\mathbb{Q}} \rightarrow \overline{\mathbb{Q}}^*$ . When  $M_{\beta'} = M_\beta$ , we see that  $\rho_{C,\beta',\pi} = \chi \otimes \rho_{C,\beta,\pi}$  are twists of each other, as are  $A_{\beta'}$  and  $A_\beta$ .

We say that a  $\mathbb{Q}$ -curve  $C$  is modular if for some positive integer  $N$  it is the quotient over  $\overline{\mathbb{Q}}$  of  $J_1(N)$ . If a  $\mathbb{Q}$ -curve  $C$  is modular, then there is a newform  $f \in S_2(\Gamma_0(N), \epsilon^{-1})$  such that  $A_f$  is an abelian variety defined over  $\mathbb{Q}$  of  $\mathrm{GL}_2$  type attached to  $C$ . This follows because  $J_1(N)$  decomposes into product of  $A_f$ 's up to isogeny over  $\mathbb{Q}$  [29]. By Proposition 10,  $A_f$  is isogenous to  $A_\beta$  for some splitting map  $\beta$ , and hence for some splitting map  $\beta$  for  $C$  we have that  $\rho_{C,\beta,\pi} \cong \rho_{f,\pi}$  for some newform  $f \in S_2(\Gamma_0(N), \epsilon^{-1})$ . Since any two splitting maps differ by a character, we see that for every splitting map  $\beta$  we have that  $\rho_{C,\beta,\pi} \cong \rho_{f,\pi}$  for some  $f \in S_2(\Gamma_0(N), \epsilon^{-1})$ . Conversely, if  $\rho_{C,\beta,\pi} \cong \rho_{f,\pi}$  for some newform  $f \in S_2(\Gamma_0(N), \epsilon^{-1})$ , then  $A_\beta$  is isogenous over  $\mathbb{Q}$  to  $A_f$  and hence the  $\mathbb{Q}$ -curve  $C$  is modular.

In summary, we have shown that  $\rho_{C,\beta,\pi} \cong \rho_{f,\pi}$  for some  $f \in S_2(\Gamma_0(N), \epsilon^{-1})$  if and only if the  $\mathbb{Q}$ -curve  $C$  is modular.

### 3. $\mathbb{Q}$ -CURVES ARISING FROM THE EQUATION $a^2 + b^{2p} = c^5$

Let  $p$  be an odd prime. Suppose  $(a, b, c) \in \mathbb{Z}^3$  satisfies  $a^2 + b^{2p} = c^5$  with  $(a, b, c) = 1$  and  $ab \neq 0$ . Recall that Lemma 3 tells us that there exists  $(s, t) \in \mathbb{Z}^2$  with  $(s, t) = 1$ ,  $st \neq 0$ , and such that

- $s^2 - 10st + 5t^2 = 5^j \gamma^p$  where  $5 \nmid \gamma$
- $v = \beta^p$  and  $j = 0$  or  $v = 5^{kp-1} \beta^p$  and  $j = 1$ , where  $5 \nmid \beta$  and  $k \geq 1$
- $s = v^2, t = u^2$ .

Consider the elliptic curve  $E^s$  defined over  $\mathbb{Q}(\sqrt{5})$  given by

$$(2) \quad E^s : Y^2 = X^3 - 3\delta \left( (3 + 2\sqrt{5})s - 3t \right) X + 4v \left( (17 - 4\sqrt{5})s - (45 - 18\sqrt{5})t \right).$$

Then

$$(3) \quad \Delta_{E^s} = 2^6 \cdot 3^6 \cdot \eta^{-3} \cdot \left( s - (5 + 2\sqrt{5})t \right)^2 \left( s - (5 - 2\sqrt{5})t \right)$$

and

$$(4) \quad j_{E^s} = \frac{2^6 \cdot 5\sqrt{5} \cdot \eta \cdot \left( (3 + 2\sqrt{5})s - 3t \right)^3}{\left( s - (5 + 2\sqrt{5})t \right)^2 \left( s - (5 - 2\sqrt{5})t \right)},$$

where  $\delta = \frac{-5+3\sqrt{5}}{2}$ ,  $\eta = \kappa^{-3}$ , and  $\kappa = \frac{-1+\sqrt{5}}{2}$

The  $\mathbb{Q}$ -curve  $E^s$  has the preconditions required to be a candidate Frey curve for solving the constraints that  $s$  is a square and  $s^2 - 10st + 5t^2$  is a  $p$ -power up to  $S$ -units for a finite set of primes  $S$ , using the modular method.

Consider in addition the elliptic curve  $E^t$  defined over  $\mathbb{Q}(\sqrt{5})$  given by

$$(5) \quad E^t : Y^2 = X^3 - 3 \cdot 2^2 \cdot \sqrt{5} \left( 3s - (15 - 10\sqrt{5})t \right) X + 2^5 \cdot 5u \left( 9s - (45 - 14\sqrt{5})t \right).$$

Then

$$(6) \quad \Delta_{E^t} = 2^{12} \cdot 3^6 \cdot 5\sqrt{5} \cdot \left( s - (5 + 2\sqrt{5})t \right)^2 \left( s - (5 - 2\sqrt{5})t \right)$$

and

$$(7) \quad j_{E^t} = \frac{64(3s - (15 - 10\sqrt{5})t)^3}{\left( s - (5 + 2\sqrt{5})t \right)^2 \left( s - (5 - 2\sqrt{5})t \right)}.$$

The  $\mathbb{Q}$ -curve  $E^t$  has the preconditions required to be a candidate Frey curve for solving the constraints that  $t$  is a square and  $s^2 - 10st + 5t^2$  is a  $p$ -power up to  $S$ -units for a finite set of primes  $S$ , using the modular method.

The superscript in  $E^s$  and  $E^t$  are intended to label the two different Frey curves attached to a solution.

**Proposition 13.** *Assume  $s/t \in \mathbb{Q}$ . The  $j$ -invariant of  $E^s$  does not lie in  $\mathbb{Q}$  unless*

- $s/t = 0, j = 1728$
- $s/t = 1, j = 8000$

*Proof.* The  $j$ -invariant of  $E^s$  lies in  $\mathbb{Q}(\sqrt{5})$ , so is of the form  $\alpha + \beta\sqrt{5}$ . Setting  $\beta = 0$  gives a system of equations which can be solved in MAPLE.  $\square$

**Proposition 14.** *Assume  $s/t \in \mathbb{Q}$ . The  $j$ -invariant of  $E^t$  does not lie in  $\mathbb{Q}$  unless*

- $s/t = \infty, j = 1728$
- $s/t = 5, j = 8000$ .

*Proof.* The  $j$ -invariant of  $E^t$  lies in  $\mathbb{Q}(\sqrt{5})$ , so is of the form  $\alpha + \beta\sqrt{5}$ . Setting  $\beta = 0$  gives a system of equations which can be solved in MAPLE.  $\square$

The elliptic curves with complex multiplication by an imaginary quadratic order  $\mathcal{O}$  of class number 2 are listed below (c.f. [24], [37]).

$d(\mathcal{O})$	$j$
-15	$(-191025 \pm 85995\sqrt{5})/2$
-20	$632000 \pm 282880\sqrt{5}$
-24	$2417472 \pm 1707264\sqrt{2}$
-35	$-58982400 \pm 26378240\sqrt{5}$
-40	$212846400 \pm 95178240\sqrt{5}$
-51	$-2770550784 \pm 671956992\sqrt{17}$
-52	$3448440000 \pm 956448000\sqrt{13}$
-88	$3147421320000 \pm 2225561184000\sqrt{2}$
-91	$-5179536506880 \pm 1436544958464\sqrt{13}$
-115	$-213932305612800 \pm 95673435586560\sqrt{5}$
-123	$-677073420288000 \pm 105741103104000\sqrt{41}$
-148	$19830091900536000 \pm 3260047059360000\sqrt{37}$
-187	$-2272668190894080000 \pm 551203000178688000\sqrt{17}$
-232	$302364978924945672000 \pm 56147767009798464000\sqrt{29}$
-235	$-411588709724712960000 \pm 184068066743177379840\sqrt{5}$
-267	$-9841545927039744000000 \pm 1043201781864732672000\sqrt{89}$
-403	$-1226405694614665695989760000 \pm 340143739727246741938176000\sqrt{13}$
-427	$-7805727756261891959906304000 \pm 999421027517377348595712000\sqrt{61}$

**Proposition 15.** *Assume  $s/t \in \mathbb{Q}$ . The elliptic curve  $E^s$  does not have complex multiplication unless*

- $s/t = 0, j = 1728, d(\mathcal{O}) = -4$
- $s/t = 1, j = 8000, d(\mathcal{O}) = -8$
- $s/t = 1/2, j = 632000 - 282880\sqrt{5}, d(\mathcal{O}) = -20$
- $s/t = 9, j = 212846400 + 95178240\sqrt{5}, d(\mathcal{O}) = -40$
- $s/t = 9/17, j = 212846400 - 95178240\sqrt{5}, d(\mathcal{O}) = -40$
- $s/t = \infty, j = 632000 + 282880\sqrt{5}, d(\mathcal{O}) = -20$

*Proof.* As the  $j$ -invariant of  $E^s$  lies in  $\mathbb{Q}(\sqrt{5})$ , we see that if  $E^s$  has complex multiplication, then the ring of its endomorphisms defined over  $\mathbb{Q}$  is an imaginary quadratic order  $\mathcal{O}$  of class number 1 or 2. In the former case,  $j(E^s) \in \mathbb{Q}$ . In the latter case, the discriminant of  $\mathcal{O}$  is one of  $d(\mathcal{O}) = -15, -20, -35, -40, -115, -235$ . For each of the corresponding values of the  $j$ -invariant, we can use MAPLE to compute the possible values for  $s/t \in \mathbb{Q}$ .  $\square$

**Proposition 16.** *Assume  $s/t \in \mathbb{Q}$ . The elliptic curve  $E^t$  does not have complex multiplication unless*

- $s/t = 5, j = 8000, d(\mathcal{O}) = -8$
- $s/t = 10, j = 632000 + 282880\sqrt{5}, d(\mathcal{O}) = -20$
- $s/t = 0, j = 632000 - 282880\sqrt{5}, d(\mathcal{O}) = -20$
- $s/t = 85/9, j = 212846400 + 95178240\sqrt{5}, d(\mathcal{O}) = -40$
- $s/t = 5/9, j = 212846400 - 95178240\sqrt{5}, d(\mathcal{O}) = -40$
- $s/t = \infty, j = 1728$

*Proof.* As the  $j$ -invariant of  $E^t$  lies in  $\mathbb{Q}(\sqrt{5})$ , we see that if  $E^t$  has complex multiplication, then the ring of its endomorphisms defined over  $\mathbb{Q}$  is an imaginary quadratic order  $\mathcal{O}$  of class number 1 or 2. In the former case,  $j(E^t) \in \mathbb{Q}$ . In the latter case, the discriminant of  $\mathcal{O}$  is one of  $d(\mathcal{O}) = -15, -20, -35, -40, -115, -235$ . For each of the corresponding values of the  $j$ -invariant, we can use MAPLE to compute the possible values for  $s/t \in \mathbb{Q}$ .  $\square$

**Corollary 17.** *If  $s, t$  satisfy the conditions from Lemma 3, then  $E^s$  does not have complex multiplication unless*

- $s/t = 0, j = 1728, d(\mathcal{O}) = -4$
- $s/t = \infty, j = 632000 + 282880\sqrt{5}, d(\mathcal{O}) = -20$

*Proof.* We eliminate the cases  $s/t = 9, j = 212846400 + 95178240\sqrt{5}, d(\mathcal{O}) = -40$  and  $s/t = 1, j = 8000, d(\mathcal{O}) = -8$  because  $p$  is an odd prime (cf. Lemma 4). The other cases are eliminated because  $s/t$  is a square.  $\square$

**Corollary 18.** *If  $s, t$  satisfy the conditions from Lemma 3, then  $E^t$  does not have complex multiplication unless*

- $s/t = 0, j = 632000 + 282880\sqrt{5}, d(\mathcal{O}) = -20$
- $s/t = \infty, j = 1728, d(\mathcal{O}) = -4$

*Proof.* The other cases are eliminated because  $s/t$  is a square.  $\square$

Assume that  $s, t$  satisfy the conditions from Lemma 3. The elliptic curves  $E^s, E^t$  are  $\mathbb{Q}$ -curves defined over  $\mathbb{Q}(\sqrt{5}, \sqrt{2})$  as long as  $s/t \neq 0, \infty$  by Corollary 17 and 18. We note that  $E = E^s, E^t$  is not a  $\mathbb{Q}$ -curve defined over  $\mathbb{Q}(\sqrt{5})$  because the 2-isogeny between  $E$  and its conjugate under  $\sqrt{5} \mapsto -\sqrt{5}$  cannot in general be defined over  $\mathbb{Q}(\sqrt{5})$ .

#### 4. SPLITTING MAPS AND MODELS OF $\mathbb{Q}$ -CURVES

Let  $E = E^s$  or  $E^t$ . We have constructed representations  $\hat{\rho}_{E, \beta, \pi} : G_{\mathbb{Q}} \rightarrow \mathrm{GL}_2(M_{\beta, \pi})$  attached to the  $\mathbb{Q}$ -curve  $E$ . However, the construction depends on a choice of splitting map  $\beta : G_{\mathbb{Q}} \rightarrow \overline{\mathbb{Q}}^*$  for  $E$ , which is related to picking a  $\mathbb{Q}$ -curve  $E'$  defined over  $K'$  in the  $\overline{\mathbb{Q}}$ -isomorphism class of  $E$  such that the decomposition of  $\mathrm{Res}_{\mathbb{Q}}^{K'} E'$  up to isogeny over  $\mathbb{Q}$  is a product of non-isogenous abelian varieties of  $\mathrm{GL}_2$ -type (see previous discussion in Section 2).

Let  $G_{\mathbb{Q}(\sqrt{5})/\mathbb{Q}} = \{\sigma_1, \sigma_5\}$ . There is a 2-isogeny  ${}^{\sigma_5}E \rightarrow E$  defined over  $\mathbb{Q}(\sqrt{5}, \sqrt{2})$ , whence we set  $\mu_E(\sigma_5)$  to be this isogeny and  $\mu_E(\sigma_1) = 1$ . The cocycle  $c_E(\sigma, \tau) = \mu_E(\sigma)^\sigma \mu_E(\tau) \mu_E(\sigma\tau)^{-1}$  can also be described as arising from a cocycle  $\alpha_E \in H^1(G_{\mathbb{Q}}, \overline{\mathbb{Q}}^*/\mathbb{Q}^*)$  given by  $\mu_E(\sigma)^*(\omega_E) = \alpha_E(\sigma)\omega_{E'}$ , with  $\omega_E, \omega_{E'}$  being the invariant differentials on  $E, E' = {}^\sigma E$ , through the formula

$$c_E(\sigma, \tau) = \alpha_E(\sigma)^\sigma \alpha_E(\tau) \alpha_E(\sigma\tau)^{-1},$$

which results from the map

$$H^1(G_{\mathbb{Q}}, \overline{\mathbb{Q}}^*/\mathbb{Q}^*) \rightarrow H^2(G_{\mathbb{Q}}, \mathbb{Q}^*),$$

which is derived from the short exact sequence

$$1 \rightarrow \mathbb{Q}^* \rightarrow \overline{\mathbb{Q}}^* \rightarrow \overline{\mathbb{Q}}^*/\mathbb{Q}^* \rightarrow 1.$$

Explicitly,

$$\begin{aligned} \alpha_{E^s}(\sigma_1) &= 1 \\ \alpha_{E^s}(\sigma_5) &= \frac{1 + \sqrt{5}}{\sqrt{2}} \\ \alpha_{E^t}(\sigma_1) &= 1 \\ \alpha_{E^t}(\sigma_5) &= \sqrt{2}. \end{aligned}$$

This can be computed using the discussion in [27, p. 288].

Consider first  $E = E^s$ . Let  $G_{\mathbb{Q}(\sqrt{5}, \sqrt{2})/\mathbb{Q}} = \{\sigma_1, \sigma_2, \sigma_5, \sigma_{10}\}$ . Then  $c_E(\sigma, \tau)$  factors through this group and has the representative values

$$\begin{aligned} c_E(\sigma_2, \sigma_2) &= 1 \\ c_E(\sigma_{10}, \sigma_{10}) &= 2 \\ c_E(\sigma_2, \sigma_{10}) &= -c_E(\sigma_{10}, \sigma_2). \end{aligned}$$

It follows that  $\mathcal{R}_E \cong M_2(\mathbb{Q})$  and hence  $\text{Res}_{\mathbb{Q}}^{\mathbb{Q}(\sqrt{5}, \sqrt{2})} E$  is isogenous over  $\mathbb{Q}$  to  $B \times B$  where  $B$  is an abelian surface defined over  $\mathbb{Q}$  with  $\text{End}_{\mathbb{Q}} B = \mathbb{Q}$ . This means that taking  $K' = \mathbb{Q}(\sqrt{5}, \sqrt{2})$  and  $E' = E$  is not a suitable choice for our purposes because the decomposition of  $\text{Res}_{\mathbb{Q}}^{\mathbb{Q}(\sqrt{5}, \sqrt{2})} E$  up to isogeny over  $\mathbb{Q}$  does not include any abelian varieties of  $\text{GL}_2$ -type.

**Proposition 19.** *The map on cocycles given by*

$$c(\sigma, \tau) \mapsto (\text{sgn } c(\sigma, \tau), |c(\sigma, \tau)|)$$

*induces an isomorphism*

$$H^2(G_{\mathbb{Q}}, \mathbb{Q}^*)[2] \rightarrow H^2(G_{\mathbb{Q}}, \{\pm 1\}) \times H^2(G_{\mathbb{Q}}, P/P^2)$$

*where  $P$  is the group of positive rational numbers.*

*Proof.* cf. [27, p. 294]. □

We call  $c^{\pm}(\sigma, \tau) = \text{sgn } c(\sigma, \tau)$  the sign component of  $c(\sigma, \tau)$ .

**Proposition 20.** *The sign component  $c_E^{\pm}(\sigma, \tau) \in H^2(G_{\mathbb{Q}}, \{\pm 1\})$  of  $c_E(\sigma, \tau)$  is given by the quaternion algebra  $(5, 2) \in H^2(G_{\mathbb{Q}}, \{\pm 1\})$ .*

*Proof.* Let  $d(\sigma) = \deg \mu_E(\sigma)$  be the degree map. In the terminology of [27, p. 294], we have that  $\{a_1\} = \{5\}$  and  $\{d_1\} = \{2\}$  are dual bases with respect to  $d(\sigma)$ . The conclusion then follows from [27, Theorem 3.1].  $\square$

Let  $\epsilon : G_{\mathbb{Q}} \rightarrow \overline{\mathbb{Q}}^*$  be a character and let  $\theta_\epsilon(\sigma, \tau) = \sqrt{\epsilon(\sigma)}\sqrt{\epsilon(\tau)}\sqrt{\epsilon(\sigma\tau)}^{-1}$ . Then  $\theta_\epsilon(\sigma, \tau) \in H^2(G_{\mathbb{Q}}, \{\pm 1\})$ .

**Proposition 21.** *Let  $\beta(\sigma) = \sqrt{\epsilon(\sigma)}\sqrt{d(\sigma)}$ . Then  $\beta(\sigma)$  is a splitting map for  $E$  if and only if  $\theta_\epsilon(\sigma, \tau) = c_E^\pm(\sigma, \tau)$  as classes in  $H^2(G_{\mathbb{Q}}, \{\pm 1\})$ .*

*Proof.* cf. [27, Theorem 4.2].  $\square$

**Proposition 22.** *We have that  $\theta_\epsilon(\sigma, \tau) = c_E^\pm(\sigma, \tau)$  as classes in  $H^2(G_{\mathbb{Q}}, \{\pm 1\})$  if and only if  $\theta_\epsilon(\sigma, \tau) = c_E^\pm(\sigma, \tau)$  as classes in  $H^2(G_{\mathbb{Q}_p}, \{\pm 1\})$  for all finite primes  $p$ .*

*Proof.* cf. [27, p. 302].  $\square$

**Proposition 23.**  *$H^2(G_{\mathbb{Q}_p}, \{\pm 1\}) \cong \{\pm 1\}$  for all finite primes  $p$ .*

*Proof.* This follows from the fact that  $H^2(G_{\mathbb{Q}_p}, \{\pm 1\})$  is contained in the 2-torsion of  $H^2(G_{\mathbb{Q}_p}, \overline{\mathbb{Q}_p}^*)$  which can be identified with isomorphism classes of simple algebras over  $\mathbb{Q}_p$  with center  $\mathbb{Q}_p$  and dimension 4 over  $\mathbb{Q}_p$ , namely, quaternion algebras over  $\mathbb{Q}_p$  (c.f. [31, Chapitre X, §5, Chapitre XIII, §4]). It is also known that over  $\mathbb{Q}_p$ , there are precisely two isomorphism classes of quaternion algebras (c.f. [38, Theorem 1.1]).  $\square$

**Proposition 24.** *We have that  $\theta_\epsilon(\sigma, \tau)_p = \epsilon_p(-1)$  as classes in  $H^2(G_{\mathbb{Q}_p}, \{\pm 1\}) \cong \{\pm 1\}$ .*

*Proof.* cf. [27, p. 302].  $\square$

The above results imply that a possible choice of splitting map  $\beta$  for  $E$  is given by

$$(8) \quad \beta(\sigma) = \sqrt{\epsilon(\sigma)}\sqrt{d(\sigma)},$$

where  $d(\sigma) = \deg \mu_E(\sigma)$ ,  $\epsilon = \epsilon_4\epsilon_5$ , and  $\epsilon_4$  is the non-trivial character of  $(\mathbb{Z}/4\mathbb{Z})^*$ , and  $\epsilon_5$  is a non-trivial character of  $(\mathbb{Z}/5\mathbb{Z})^*$ . For this choice of  $\beta$ , we have that  $\epsilon_\beta = \epsilon$  and  $M_\beta = \mathbb{Q}(i)$ . The character  $\epsilon$  has kernel  $\{\pm 1\}$ , regarded as a character of  $(\mathbb{Z}/20\mathbb{Z})^\times$ . To fix choices, let us suppose that  $\epsilon(\pm 3) = i \in \mathbb{C}$ .

Explicitly, the coboundary relating the cocycles  $c_E(\sigma, \tau)$  and  $c_\beta(\sigma, \tau) = \beta(\sigma)\beta(\tau)\beta(\sigma\tau)^{-1}$  can be described as follows. We will use this coboundary to find a  $\mathbb{Q}$ -curve  $E_\beta$  defined over a number field  $K_\beta$  in the  $\overline{\mathbb{Q}}$ -isomorphism class of  $E$  such that  $c_{E_\beta}(\sigma, \tau) = c_\beta(\sigma, \tau)$  as cocycles (not just as classes).

Let  $\alpha_1(\sigma) = \alpha_E(\sigma) \frac{\sigma\sqrt{\gamma_1}}{\sqrt{\gamma_1}}$ , where  $\gamma_1 = \frac{5+\sqrt{5}}{2}$ . Then we have that

$$\begin{aligned}\alpha_1(\sigma_1) &= 1 \\ \alpha_1(\sigma_5) &= \sqrt{2}.\end{aligned}$$

Recall that the cocycles  $\alpha(\sigma)$ ,  $\alpha_1(\sigma)$  have values in  $\overline{\mathbb{Q}}^*/\mathbb{Q}^*$  so any equality is regarded up to multiplication by an element in  $\mathbb{Q}^*$  (in this case, by  $\pm 1$ ).

We wish to find a  $\gamma_2$  such that

$$(9) \quad \alpha_2(\sigma) = \alpha_1(\sigma) \sqrt{\frac{\sigma\gamma_2}{\gamma_2}}$$

satisfies

$$c_\beta(\sigma, \tau) = \alpha_2(\sigma)^\sigma \alpha_2(\tau) \alpha_2(\sigma\tau)^{-1}.$$

Let  $K_\beta = \mathbb{Q}(z)$  where  $z = \sqrt{\frac{5+\sqrt{5}}{2}}$  is a root of  $X^4 - 5X^2 + 5$  and let  $G_{K_\beta/\mathbb{Q}} = \{\sigma_1^\pm, \sigma_5^\pm\}$ . The unit group of  $K_\beta$  is generated by

$$\begin{aligned}u_1 &= -1 \\ u_2 &= 2 - z^2 \\ u_3 &= -z^2 + z + 2 \\ u_4 &= -z^3 + z^2 + 3z - 3\end{aligned}$$

and is isomorphic to  $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z} \times \mathbb{Z} \times \mathbb{Z}$ .

Let  $g = \alpha_2(\sigma_5^+)$ . Then  $\frac{g^2}{2} = \frac{\sigma_5^+ \gamma_2}{\gamma_2}$  is a necessary constraint on  $g$  using Equation (9). As an initial guess, let us suppose that  $\frac{g^2}{2} = u$  is a unit in  $K_\beta$ . This unit  $u = 2 - z$  can be obtained by noting  $(2) = (g^2)$  in  $K_\beta$ . Since  $N_{K_\beta/\mathbb{Q}}(u) = 1$ , by Hilbert 90, there is a  $\gamma_2 \in K_\beta$  such that  $\frac{\sigma\gamma_2}{\gamma_2} = u$ , where  $\sigma = \sigma_5^+$ . This  $\gamma_2$  can be obtained from the expression

$$\gamma_2' = z + uz^\sigma + u^{1+\sigma}z^{\sigma^2} + u^{1+\sigma+\sigma^2}z^{\sigma^3}$$

used in the proof of Hilbert 90. Then up to scaling by an element in  $\mathbb{Q}^*$ , we may take  $\gamma_2 = \frac{1}{\gamma_2'} = z^3 + z^2 - 2z$ .

Finally, if we let  $\alpha_2(\sigma) = \alpha_E(\sigma)\sqrt{\frac{\sigma\gamma}{\gamma}}$  where

$$\begin{aligned}\gamma &= z^2(z^3 + z^2 - 2z) \\ &= 3z^3 + 5z^2 - 5z - 5 \\ &= z^3/u_3,\end{aligned}$$

then the cocycle in  $H^2(G_{\mathbb{Q}}, \mathbb{Q}^*)$  arising from  $\alpha_2(\sigma)$  is precisely  $c_{\beta}(\sigma, \tau) = \beta(\sigma)\beta(\tau)\beta(\sigma\tau)^{-1}$ . For this fact, we list for convenience the following values

$$\begin{aligned}\frac{\sigma_5^+ \gamma}{\gamma} &= \frac{g^2}{2}, \\ \frac{\sigma_5^- \gamma}{\gamma} &= \frac{g^2}{2} \frac{1}{u_4^2}, \\ \frac{\sigma_1^+ \gamma}{\gamma} &= 1, \\ \frac{\sigma_1^- \gamma}{\gamma} &= u_3^2,\end{aligned}$$

which show that  $\alpha_2(\sigma)$  has values in  $K_{\beta}$ .

Let  $E_{\beta}$  be the  $\mathbb{Q}$ -curve defined over  $K_{\beta}$  in the  $\overline{\mathbb{Q}}$ -isomorphism class of  $E$  given by

$$(10) \quad \begin{aligned}Y^2 &= X^3 - 3\delta \left( (3 + 2\sqrt{5})s - 3t \right) \gamma^2 X \\ &\quad + 4v \left( (17 - 4\sqrt{5})s - (45 - 18\sqrt{5})t \right) \gamma^3.\end{aligned}$$

Then

$$\Delta_{E_{\beta}} = 2^6 \cdot 3^6 \cdot \eta^{-3} \cdot \left( s - (5 + 2\sqrt{5})t \right)^2 \left( s - (5 - 2\sqrt{5})t \right) \gamma^6,$$

where  $\delta = \frac{-5+3\sqrt{5}}{2}$ ,  $\eta = \kappa^{-3}$ , and  $\kappa = \frac{-1+\sqrt{5}}{2} = -1/u_2$ .

Let  $\alpha_{E_{\beta}}(\sigma)$  be the cocycle in  $H^1(G_{\mathbb{Q}}, \overline{\mathbb{Q}}^*/\mathbb{Q}^*)$  given by  $\mu_{E_{\beta}}(\sigma)^*(\omega_{E_{\beta}}) = \alpha_{E_{\beta}}(\sigma)\omega_{E'_{\beta}}$  where  $E'_{\beta} = {}^{\sigma}E_{\beta}$ . From consideration of how twisting affects the  $\alpha_E(\sigma)$  [27, p. 291], we have that

$$(11) \quad \alpha_{E_{\beta}}(\sigma) = \alpha_E(\sigma) \frac{\sigma\sqrt{\gamma}}{\sqrt{\gamma}} = \alpha_2(\sigma)\xi(\sigma)$$

where  $\xi(\sigma) \in \{\pm 1\}$ . Replacing the choices of  $\mu_{E_{\beta}}(\sigma)$  for  $E_{\beta}$  (which result from  $E_{\beta}$  being a twist of  $E$ ) by  $\mu_{E_{\beta}}(\sigma)\xi(\sigma)$ , we get a choice of  $\mu_{E_{\beta}}(\sigma)$ 's for  $E_{\beta}$  which are locally constant on  $G_{K_{\beta}}$  and such that the values  $\alpha_2(\sigma)$  lie in

$K_\beta$ . Hence, if we use  $E_\beta$  instead of  $E$ , then  $E_\beta$  is a  $\mathbb{Q}$ -curve defined over  $K_\beta$  and we have that

$$c_{E_\beta}(\sigma, \tau) = c_\beta(\sigma, \tau) = \beta(\sigma)\beta(\tau)\beta(\sigma\tau)^{-1}$$

as cocycles.

Now work of Quer [27, Theorem 5.4, Case (2)] implies that

$$\mathrm{Res}_{\mathbb{Q}}^{K_\beta} E_\beta \sim_{\mathbb{Q}} A_\beta \times A_{\beta'},$$

where  $A_\beta, A_{\beta'}$  are abelian varieties defined over  $\mathbb{Q}$  of  $\mathrm{GL}_2$ -type with endomorphism algebra  $\mathbb{Q}(i)$ . Here,  $\beta' = \chi \cdot \beta$  is a splitting map such that  $\epsilon_{\beta'} = \epsilon$  and  $\chi = \left(\frac{\cdot}{5}\right)$  is the quadratic character attached to  $\mathbb{Q}(\sqrt{5})$ .

A similar calculation can be made for  $E = E^t$  with exactly the same  $\beta$  as above but  $\gamma = z^3 + z^2 - 2z$ . For this, it is convenient to simply note that  $\alpha_{E^t}(\sigma) = \alpha_1(\sigma)$ .

**Proposition 25.** *The elliptic curve  $E = E^s$  (resp.  $E = E^t$ ) has the following properties.*

- *$E$  has potentially good ordinary reduction in characteristic 3 if  $s \not\equiv 0 \pmod{3}$  (resp.  $t \not\equiv 0 \pmod{3}$ ) and potentially good supersingular reduction in characteristic 3 if  $s \equiv 0 \pmod{3}$  (resp.  $t \equiv 0 \pmod{3}$ ).*
- *The sign component  $c_E^\pm(\sigma, \tau) = \mathrm{sgn} \mu_E(\sigma)^\sigma \mu_E(\tau) \mu_E(\sigma\tau)^{-1} \in H^2(G_{\mathbb{Q}}, \{\pm 1\})$  is trivial when restricted to  $G_{\mathbb{Q}_3}$ .*

*Proof.* The elliptic curve  $E$  has potentially good reduction because the denominator of its  $j$ -invariant is not divisible by a prime above 3 by Equation (4) and (7) and Lemma 5. Its  $j$ -invariant is zero in characteristic 3 if and only if  $s \equiv 0 \pmod{3}$  (resp.  $t \equiv 0 \pmod{3}$ ) so  $E$  is supersingular in characteristic 3 if and only if  $s \equiv 0 \pmod{3}$  (resp.  $t \equiv 0 \pmod{3}$ ). Since the sign component  $c_E^\pm(\sigma, \tau)$  is given by the quaternion algebra (5, 2) by Proposition 20, we see that it is trivial when restricted to  $G_{\mathbb{Q}_3}$ .  $\square$

**Theorem 26.** *The abelian varieties  $A_\beta$  and  $A_{\beta'}$  are modular.*

*Proof.* In the case of potentially good ordinary reduction,  $E$  satisfies the hypotheses of [15, Theorem 5.1] because of Proposition 25 so we deduce that it is modular. In the case of potentially good supersingular reduction, we note that  $\mathbb{P}\rho_{E, \beta, \pi}$  is unramified at 3 so by [15, Theorem 5.2] we also deduce that  $E$  is modular.  $\square$

The abelian varieties  $A_\beta$  and  $A_{\beta'}$  are not isogenous over  $\mathbb{Q}$  since  $\beta' \neq \sigma\beta$  for any  $\sigma \in G_{\mathbb{Q}}$ . Let  $f$  and  $f'$  be the newforms attached to  $A_\beta$  and  $A_{\beta'}$  respectively.

**Theorem 27.**  *$A_{\beta'}$  is isogenous over  $\mathbb{Q}$  to a twist of  $A_\beta$  by  $\chi^{-1} = \chi = \left(\frac{5}{\cdot}\right)$  and hence  $f'$  is a twist of  $f$  by  $\chi^{-1} = \chi = \left(\frac{5}{\cdot}\right)$ .*

*Proof.* This can be seen from the Galois action on the Tate module of  $A_\beta$  and  $A_{\beta'}$  which is given by

$$\begin{aligned} x \otimes y &\mapsto x \cdot \beta(\sigma)^{-1} \otimes \mu_E(\tau)(\tau(y)) \\ x \otimes y &\mapsto x \cdot \beta'(\sigma)^{-1} \otimes \mu_E(\tau)(\tau(y)). \end{aligned}$$

Since  $\beta' = \chi \cdot \beta$ , we see that

$$\hat{\rho}_{A,\beta',\pi}(\sigma) = \epsilon^{-1}(\sigma)\hat{\rho}_{A,\beta,\pi}(\sigma),$$

where  $\pi$  is a prime of  $M_{\beta'} = M_\beta = \mathbb{Q}(i)$  above  $p$ . □

## 5. SERRE INVARIANTS ATTACHED TO $\mathbb{Q}$ -CURVES

For  $E = E^s$  or  $E^t$ , let

$$\rho_{E,\beta,\pi} : G_{\mathbb{Q}} \rightarrow \overline{\mathbb{F}}_p^* \mathrm{GL}_2(\mathbb{F}_p)$$

be the reduction of  $\hat{\rho}_{E,\beta,\pi}$ . Assume that this reduction is irreducible. We now determine the character, conductor, and weight of  $\rho_{E,\beta,\pi}$  from the relation between  $E$  and  $E_\beta$ .

The discriminant of  $K_\beta$  is given by  $d_{K_\beta/\mathbb{Q}} = 2^4 \cdot 5^3 = 2000$ . The prime factorizations of (2), (3), and (5) in  $K_\beta$  are given as follows

$$\begin{aligned} (2) &= \mathfrak{q}_2^2 \\ (3) &= \mathfrak{q}_3 \\ (5) &= \mathfrak{q}_5^4. \end{aligned}$$

Let  $\nu_2 = -2 + 3z + z^2 - z^3$ ,  $\nu_3 = 3$ ,  $\nu_5 = z$  be uniformizers for  $\mathfrak{q}_2, \mathfrak{q}_3, \mathfrak{q}_5$  whose associated valuations are denoted  $v_2(\cdot), v_3(\cdot), v_5(\cdot)$ .

Let  $M$  be a number field. For a prime  $\pi$  of  $M$ , let  $\hat{V}_\pi$  be a free  $M_\pi$ -module of rank  $n$  with a continuous  $M_\pi$ -linear action of  $G_K$ . A collection  $\{\hat{V}_\pi\}$  of such  $\hat{V}_\pi$ 's where  $\pi$  runs through all primes of  $M$  is called a system of  $M_\pi[G_K]$ -modules.

Let  $A$  be an abelian variety of dimension  $g$  defined over  $K$  with endomorphism algebra equal to a number field  $M$ . The  $p$ -adic Tate module  $\hat{V}_p(A)$  of  $A$  is isomorphic to  $M_p^d$ , where  $M_p = M \otimes \mathbb{Q}_p = \prod_{\pi|p} M_\pi$  and  $[M : \mathbb{Q}]d = 2g$ . The  $\pi$ -adic Tate module  $\hat{V}_\pi(A)$  of  $A$  is isomorphic to  $M_\pi^d$  and can be obtained as  $\hat{V}_\pi(A) = \hat{V}_p(A) \otimes_{M_p} M_\pi$ , where  $M_\pi$  is regarded as a  $M_p$ -module under the projection  $M_p \rightarrow M_\pi$ .

For each prime  $\pi$  of  $M$ , there exists an  $M_\pi$ -basis for  $\hat{V}_\pi$  such that the  $\mathcal{O}_\pi$ -module  $\Lambda_\pi$  generated by this basis is  $G_K$ -invariant. This follows from the compactness of  $G_K$  and the continuity of its action on  $\hat{V}_\pi$ . The  $k_\pi[G_K]$ -module  $\hat{V}_\pi = T_\pi/\pi T_\pi$  is called a reduction of  $\hat{V}_\pi$ . Let  $\rho_\pi : G_K \rightarrow \text{GL}(\hat{V}_\pi)$  be its associated representation.

Let  $I_K$  be the inertia subgroup of  $G_K$ , where  $K$  is a local field whose residue field has characteristic  $\ell \neq p$ . Suppose that  $\{\hat{V}_\pi\}$  is a system of  $M_\pi[G_K]$ -modules such that

- (1) there is an open subgroup of  $I_K$  such that its action on  $\hat{V}_\pi$  is unipotent
- (2) the character of  $\hat{V}_\pi$  as a  $M_\pi[G_K]$ -module has values in  $M$  which are independent of  $\pi$ .

Let  $G_i$  be the lower index ramification subgroups of  $I$  with the normalization  $G_0 = I$ .

We define the conductor exponent of  $\{\hat{V}_\pi\}$  as

$$(12) \quad e(\pi) = \text{codim}_{M_\pi} \hat{V}_\pi^{I_K} + \sum_{i=1}^{\infty} \frac{1}{[G_0 : G_i]} \text{codim}_{k_\pi} V_\pi^{G_i}$$

for any  $\pi \nmid \ell$ . This quantity is a non-negative integer which is independent of  $\pi$  from arguments found in Ogg [25], Serre-Tate [34].

Suppose that  $\{\hat{V}_\pi\}$  is a system of  $M_\pi[G_K]$ -modules, where  $K$  is a global field. We define the conductor of  $\{\hat{V}_\pi\}$  to be the ideal

$$\prod_{\lambda} \lambda^{e_\lambda},$$

where  $\lambda$  runs through all finite primes  $\lambda$  of  $K$ , and  $e_\lambda$  is the conductor exponent of  $\{\hat{V}_\pi\}$ , regarded as a system of  $M_\pi[G_{K_\lambda}]$ -modules by restriction to a decomposition group above  $\lambda$ .

**Lemma 28.** *The conductor exponent of a system of  $M_\pi[G_K]$ -modules is additive on direct sums.*

*Proof.* This follows from formula (12) defining conductor exponent.  $\square$

The conductor of an abelian variety  $A$  defined over  $K$  is defined as the conductor of the system of  $\mathbb{Q}_p[G_K]$ -modules  $\{\hat{V}_p(A)\}$ .

**Lemma 29.** *Let  $A$  be an abelian variety defined over  $K$  with endomorphism algebra equal to a number field  $M$ . Let  $N_\mathbb{Q}$  denote the conductor of  $\{\hat{V}_p(A)\}$ , regarded as a system of  $\mathbb{Q}_p[G_K]$ -modules and let  $N_M$  denote the conductor of  $\{\hat{V}_\pi(A)\}$ , regarded as a system of  $M_\pi[G_K]$ -modules. Then  $N_\mathbb{Q} = N_M^{[M:\mathbb{Q}]}$ .*

*Proof.* By results in [1, Theorem 4.3], the system of representations considered satisfy the conditions required for the definition of conductor to be independent of  $\pi$ . Let us fix a prime  $\lambda \mid \ell$  of  $K$  and then compare the conductor exponents  $e(p)$  and  $e(\pi)$  for  $\hat{V}_p = \hat{V}_p(A)$  and  $\hat{V}_\pi = \hat{V}_\pi(A)$ , considered as  $\mathbb{Q}_p[G_{K_\lambda}]$  and  $M_\pi[G_{K_\lambda}]$  modules, where  $\pi \mid p$  and  $p \neq \ell$ . Since we are free to choose  $p \neq \ell$ , we can assume without loss of generality that  $p$  is unramified in  $M$ . Let  $f_\pi = [M_\pi : \mathbb{Q}_p] = [k_\pi : \mathbb{F}_p]$  be the inertia degree of  $\pi$ . Now, we have that

$$\dim_{\mathbb{Q}_p} \hat{W} = f_\pi \dim_{M_\pi} \hat{W}$$

for a sub- $M_\pi$ -module  $\hat{W}$  of  $\hat{V}_\pi$ . Also,

$$\dim_{\mathbb{F}_p} W = f_\pi \dim_{k_\pi} W$$

for a sub- $k_\pi$ -module  $W$  of  $V_\pi$ . Since

$$\hat{V}_p(A) = \bigoplus_{\pi \mid p} \hat{V}_\pi(A),$$

it follows that  $e(p) = \sum_{\pi \mid p} f_\pi e(\pi)$ . Since the  $e(\pi)$ 's are all equal, we have that  $e(p) = [M : \mathbb{Q}]e(\pi)$ .  $\square$

**Lemma 30.** *Suppose that  $E$  and  $E'$  are elliptic curves defined by*

$$\begin{aligned} E : Y^2 + a_1XY + a_3Y &= X^3 + a_2X^2 + a_4X + a_6 \\ E' : Y^2 + a'_1XY + a'_3Y &= X^3 + a'_2X^2 + a'_4X + a'_6, \end{aligned}$$

where the  $a_i, a'_i$  lie in a discrete valuation ring  $\mathcal{O}$  with uniformizer  $\nu$ , and the Weierstrass equations are in minimal form. If  $E$  has reduction type  $I_0^*$  and  $a'_i \equiv a_i \pmod{\nu^4}$ , then  $E'$  also has reduction type  $I_0^*$ .

*Proof.* Since the Weierstrass equations for  $E$  and  $E'$  are in minimal form, when  $E$  and  $E'$  are processed through Tate's algorithm [36], the algorithm terminates at one of Steps 1–10 and does not reach Step 11 to loop back a second time. As  $E$  has reduction type  $I_0^*$ , the algorithm applied to  $E$  terminates at Step 6. Since the transformations used in Steps 1–10 are translations, they preserve the congruences  $a_i \equiv a'_i \pmod{\nu^4}$  as  $E$  and  $E'$  are processed through the algorithm, and since the conditions to exit at Steps 1–6 are congruence conditions modulo  $\nu^4$  on the coefficients of the Weierstrass equations, we see that if the algorithm applied to  $E$  terminates at Step 6, it must also terminate at Step 6 for  $E'$ .  $\square$

**Lemma 31.** *Suppose that  $E$  and  $E'$  are elliptic curves defined by*

$$\begin{aligned} E : Y^2 + a_1XY + a_3Y &= X^3 + a_2X^2 + a_4X + a_6 \\ E' : Y^2 + a'_1XY + a'_3Y &= X^3 + a'_2X^2 + a'_4X + a'_6, \end{aligned}$$

where the  $a_i, a'_i$  lie in a discrete valuation ring  $\mathcal{O}$  with uniformizer  $\nu$ , and the valuation at  $\nu$  of the discriminants is equal to 12. If  $E$  has reduction type  $II^*$  and  $a'_i \equiv a_i \pmod{\nu^6}$ , then  $E'$  also has reduction type  $II^*$ . If  $E$  has reduction type  $I_0$  and  $a'_i \equiv a_i \pmod{\nu^6}$ , then  $E'$  also has reduction type  $I_0$ .

*Proof.* As  $v(\Delta) = 12$ , when  $E$  and  $E'$  are processed through Tate's algorithm [36], the algorithm terminates at one of Steps 1–10 or reaches Step 11 to loop back a second time before terminating.

If  $E$  has reduction type  $II^*$ , the algorithm applied to  $E$  terminates at Step 10. Since the transformations used in Steps 1–10 are translations, they preserve the congruences  $a_i \equiv a'_i \pmod{\nu^6}$  as  $E$  and  $E'$  are processed through the algorithm, and since the conditions to exit at Steps 1–10 are congruence conditions modulo  $\nu^6$  on the coefficients of the Weierstrass equations, we see that if the algorithm applied to  $E$  terminates at Step 10, it must also terminate at Step 10 for  $E'$ .

If  $E$  has reduction type  $I_0$ , the algorithm applied to  $E$  reaches Step 11 to loop back a second time to terminate at Step 1 (because the valuation of the discriminant of the model for  $E$  is equal to 12). Again, since  $a'_i \equiv a_i \pmod{\nu^6}$ , it follows that the algorithm applied to  $E'$  also reaches Step 11 to

loop back a second time to terminate at Step 1 (again because the valuation of the discriminant of the model for  $E'$  is equal to 12).  $\square$

**Theorem 32.** *The conductor of  $E_\beta = E_\beta^s$  is*

$$\mathfrak{m} = \mathfrak{q}_2^\alpha \cdot \mathfrak{q}_3^2 \cdot \mathfrak{q}_5^\varepsilon \cdot \prod'_{\mathfrak{q}|s^2-10st+5t^2} \mathfrak{q},$$

where the product does not include primes dividing  $2 \cdot 3 \cdot 5$ ;  $\alpha = 0, 4$ , and  $\varepsilon = 0, 2$  according as  $s \equiv 0 \pmod{5}$ ,  $s \not\equiv 0 \pmod{5}$ .

*Proof.* Recall that  $E_\beta$  is given by

$$(13) \quad Y^2 = X^3 - 3\delta \left( (3 + 2\sqrt{5})s - 3t \right) \gamma^2 X \\ + 4v \left( (17 - 4\sqrt{5})s - (45 - 18\sqrt{5})t \right) \gamma^3,$$

with

$$(14) \quad \Delta_{E_\beta} = 2^6 \cdot 3^6 \cdot \eta^{-3} \cdot (s - (5 + 2\sqrt{5})t)^2 (s - (5 - 2\sqrt{5})t) \cdot \gamma^6,$$

where

$$\delta = \left( \frac{-5 + 3\sqrt{5}}{2} \right) \\ \eta = \kappa^{-3} \\ \kappa = \frac{-1 + \sqrt{5}}{2} \\ \gamma = z^2(z^3 + z^2 - 2z).$$

Let

$$(15) \quad c_4 = -2^4 \cdot 3 \cdot -3\delta \left( (3 + 2\sqrt{5})s - 3t \right) \gamma^2 \\ c_6 = -2^5 \cdot 3^3 \cdot 4v \left( (17 - 4\sqrt{5})s - (45 - 18\sqrt{5})t \right) \gamma^3.$$

Let  $\mathfrak{q}$  be a prime not dividing  $2 \cdot 3 \cdot 5$  but dividing  $\Delta_{E_\beta}$ . The elliptic curve  $E_\beta$  has multiplicative bad reduction at  $\mathfrak{q}$  if one of  $c_4, c_6 \not\equiv 0 \pmod{\mathfrak{q}}$ . Since  $\delta$  and  $\gamma$  are not divisible by  $\mathfrak{q}$  and  $(s, t) = 1$ , we note that  $c_4 \equiv c_6 \equiv 0 \pmod{\mathfrak{q}}$  happens if and only if

$$(3 + 2\sqrt{5})s - 3t \equiv 0 \pmod{\mathfrak{q}} \\ (17 - 4\sqrt{5})s - (45 - 18\sqrt{5})t \equiv 0 \pmod{\mathfrak{q}}.$$

But since the determinant of this linear system is  $48(2 - \sqrt{5})$ , which is not divisible by  $\mathfrak{q}$ , we see that  $c_4 \equiv c_6 \equiv 0 \pmod{\mathfrak{q}}$  if and only if  $s \equiv t \equiv 0 \pmod{\mathfrak{q}}$ , which does not happen because  $(s, t) = 1$ . Hence,  $E_\beta$  has multiplicative bad reduction at  $\mathfrak{q}$ .

If  $s \not\equiv 0 \pmod{3}$ , then  $v_3(c_4) = 2$ . If  $s \equiv 0 \pmod{3}$ , then by Equation (14) we have that  $v_3(\Delta_{E_\beta}) = 6$ . Hence, by [26, Tableaux II], Equation (13) is in minimal form at  $\mathfrak{q}_3$ . We go through all possibilities for  $(v, t)$  modulo  $\nu_3^4$ , and in each case we compute the reduction type of  $E_\beta$  at  $\mathfrak{q}_3$  using MAGMA [5], which all turn out to be type  $I_0^*$ . By Lemma 30, this determines all the possible conductor exponents for  $E_\beta$  at  $\mathfrak{q}_3$ .

We change the model for elliptic curve  $E_\beta$  by replacing  $\gamma$  by  $\mu = \gamma/z^2$  in Equation (13). This has the effect of reducing  $v_5(\Delta_{E_\beta})$  because now  $v_5(\mu) = 1$ . Note this is only done for the purposes of computing the conductor exponent at  $\mathfrak{q}_5$ , we do not actually use this modified model in the overall argument. The modified model is given by

$$(16) \quad Y^2 = X^3 - 3\delta \left( (3 + 2\sqrt{5})s - 3t \right) \mu^2 X \\ + 4v \left( (17 - 4\sqrt{5})s - (45 - 18\sqrt{5})t \right) \mu^3.$$

with

$$(17) \quad \Delta_{E_\beta} = 2^6 \cdot 3^6 \cdot \eta^{-3} \cdot (s - (5 + 2\sqrt{5})t)^2 (s - (5 - 2\sqrt{5})t) \cdot \mu^6,$$

If  $s \not\equiv 0 \pmod{5}$ , then by Equation (17), we have that  $v_5(\Delta_{E_\beta}) = 6$  so Equation (16) is minimal at  $\mathfrak{q}_5$ . We go through all possibilities for  $(v, t)$  modulo  $\nu_5^4$  subject to  $s \not\equiv 0 \pmod{5}$ , and in each case we compute the reduction type of  $E_\beta$  at  $\mathfrak{q}_5$  using MAGMA [5], which all turn out to be type  $I_0^*$ . By Lemma 30, this determines all the possible conductor exponents for  $E_\beta$  at  $\mathfrak{q}_5$ . If  $s \equiv 0 \pmod{5}$ , then  $v_5(s) \geq 4$ . It follows from Equations (15) (17) that  $v_5(c_4) \geq 4$ ,  $v_5(c_6) \geq 6$ ,  $v_5(\Delta_{E_\beta}) = 12$ . Replacing  $(X, Y)$  by  $(X\nu_5^2, Y\nu_5^3)$  yields a model for  $E_\beta$  which has good reduction at  $\mathfrak{q}_5$ .

Since  $s \not\equiv t \pmod{2}$ , then by Equation (14) we see that  $v_2(\Delta_{E_\beta}) = 12$ . We go through all possibilities for  $(v, t)$  modulo  $\nu_2^6$ , and in each case we compute the reduction type of  $E_\beta$  at  $\mathfrak{q}_2$  using MAGMA [5], which all turn out to be type  $II^*$  or  $I_0$ . By Lemma 31, this determines all the possible conductor exponents for  $E_\beta$  at  $\mathfrak{q}_2$ .  $\square$

**Theorem 33.** *The conductor of  $E_\beta = E_\beta^t$  is*

$$\mathfrak{m} = \mathfrak{q}_2^\alpha \cdot \mathfrak{q}_3^2 \cdot \mathfrak{q}_5^\varepsilon \cdot \prod'_{\mathfrak{q}|s^2-10st+5t^2} \mathfrak{q},$$

where the product does not include primes dividing  $2 \cdot 3 \cdot 5$ ;  $\alpha = 0, 4$ , and  $\varepsilon = 0, 2$  according as  $s \not\equiv 0 \pmod{5}$ ,  $s \equiv 0 \pmod{5}$ .

*Proof.* Recall that  $E_\beta$  is given by

$$(18) \quad Y^2 = X^3 - 3 \cdot 2^2 \cdot \sqrt{5} \left( 3s - (15 - 10\sqrt{5})t \right) \gamma^2 X \\ + 2^5 \cdot 5u \left( 9s - (45 - 14\sqrt{5})t \right) \gamma^3.$$

with

$$(19) \quad \Delta_{E_\beta} = 2^{12} \cdot 3^6 \cdot 5\sqrt{5} \cdot \left( s - (5 + 2\sqrt{5})t \right)^2 \left( s - (5 - 2\sqrt{5})t \right) \gamma^6$$

where

$$\gamma = z^3 + z^2 - 2z.$$

Let

$$c_4 = -2^4 \cdot 3 \cdot -3 \cdot 2^2 \cdot \sqrt{5} \left( 3s - (15 - 10\sqrt{5})t \right) \gamma^2 \\ c_6 = -2^5 \cdot 3^3 \cdot 2^5 \cdot 5u \left( 9s - (45 - 14\sqrt{5})t \right) \gamma^3.$$

Let  $\mathfrak{q}$  be a prime not dividing  $2 \cdot 3 \cdot 5$  but dividing  $\Delta_{E_\beta}$ . The elliptic curve  $E_\beta$  has multiplicative bad reduction at  $\mathfrak{q}$  if one of  $c_4, c_6 \not\equiv 0 \pmod{\mathfrak{q}}$ . Since  $\gamma$  is not divisible by  $\mathfrak{q}$  and  $(s, t) = 1$ , we note that  $c_4 \equiv c_6 \equiv 0 \pmod{\mathfrak{q}}$  happens if and only if

$$3s - (15 - 10\sqrt{5})t \equiv 0 \pmod{\mathfrak{q}} \\ 9s - (45 - 14\sqrt{5})t \equiv 0 \pmod{\mathfrak{q}}.$$

But since the determinant of this linear system is  $48\sqrt{5}$ , which is not divisible by  $\mathfrak{q}$ , we see that  $c_4 \equiv c_6 \equiv 0 \pmod{\mathfrak{q}}$  if and only if  $s \equiv t \equiv 0 \pmod{\mathfrak{q}}$ , which does not happen because  $(s, t) = 1$ . Hence,  $E_\beta$  has multiplicative bad reduction at  $\mathfrak{q}$ .

If  $t \not\equiv 0 \pmod{3}$ , then  $v_3(c_4) = 2$ . If  $t \equiv 0 \pmod{3}$ , then by Equation (19) we have that  $v_3(\Delta_{E_\beta}) = 6$ . Hence, by [26, Tableaux II], Equation (18) is in minimal form at  $\mathfrak{q}_3$ . We go through all possibilities for  $(u, s)$  modulo  $\nu_3^4$ , and in each case we compute the reduction type of  $E_\beta$  at  $\mathfrak{q}_3$  using MAGMA

[5], which all turn out to be type  $I_0^*$ . By Lemma 30, this determines all the possible conductor exponents for  $E_\beta$  at  $\mathfrak{q}_3$ .

We change the model for elliptic curve  $E_\beta$  by replacing  $\gamma$  by  $\mu = \gamma/z^2$  in Equation (13). This has the effect of reducing  $v_5(\Delta_{E_\beta})$  because now  $v_5(\mu) = -1$ . This is only done for the purposes of computing the conductor exponent at  $\mathfrak{q}_5$ . The modified model is given by

$$(20) \quad Y^2 = X^3 - 3 \cdot 2^2 \cdot \sqrt{5} \left( 3s - (15 - 10\sqrt{5})t \right) \mu^2 X \\ + 2^5 \cdot 5u \left( 9s - (45 - 14\sqrt{5})t \right) \mu^3.$$

with

$$(21) \quad \Delta_{E_\beta} = 2^{12} \cdot 3^6 \cdot 5\sqrt{5} \cdot \left( s - (5 + 2\sqrt{5})t \right)^2 \left( s - (5 - 2\sqrt{5})t \right) \mu^6.$$

If  $s \not\equiv 0 \pmod{5}$ , then  $v_5(\Delta_{E_\beta}) = 0$  so  $E_\beta$  has good reduction at  $\mathfrak{q}_5$ . If  $s \equiv 0 \pmod{5}$ , then by Equation (21), we have that  $v_5(\Delta_{E_\beta}) = 6$  so Equation (20) is minimal at  $\mathfrak{q}_5$ . We go through all possibilities for  $(u, s)$  modulo  $\nu_5^4$  subject to  $s \not\equiv 0 \pmod{5}$ , and in each case we compute the reduction type of  $E_\beta$  at  $\mathfrak{q}_5$  using MAGMA [5], which all turn out to be type  $I_0^*$ . By Lemma 30, this determines all the possible conductor exponents for  $E_\beta$  at  $\mathfrak{q}_5$ .

We change the model for elliptic curve  $E_\beta$  by replacing  $\gamma$  by  $\mu = \gamma/\nu_2^2$  in Equation (13). This has the effect of reducing  $v_2(\Delta_{E_\beta})$  because now  $v_2(\mu) = -2$ . Again, this is only done for the purposes of computing the conductor exponent at  $\mathfrak{q}_2$ .

Since  $s \not\equiv t \pmod{2}$ , then by Equation(19) we see that  $v_2(\Delta_{E_\beta}) = 12$ . We go through all possibilities for  $(u, s)$  modulo  $\nu_2^6$ , and in each case we compute the reduction type of  $E_\beta$  at  $\mathfrak{q}_2$  using MAGMA [5], which all turn out to be type  $II^*$  or  $I_0$ . By Lemma 31, this determines all the possible conductor exponents for  $E_\beta$  at  $\mathfrak{q}_2$ .  $\square$

**Theorem 34.** *The conductor of  $\text{Res}_{\mathbb{Q}}^{K_\beta} E_\beta^s$  is*

$$d_{K_\beta/\mathbb{Q}}^2 \cdot N_{K_\beta/\mathbb{Q}}(\mathfrak{m}) = 2^{8+2\alpha} \cdot 3^8 \cdot 5^{6+\varepsilon} \cdot \prod'_{q|s^2-10st+5t^2} q^4,$$

where the product does not include primes dividing  $2 \cdot 3 \cdot 5$ ;  $\alpha = 0, 4$ , and  $\varepsilon = 0, 2$  according as  $s \equiv 0 \pmod{5}$ ,  $s \not\equiv 0 \pmod{5}$ .

*Proof.* cf. [22, Lemma, p. 178]. We also note that  $K_\beta$  is unramified outside  $\{2, 5\}$  so the product is of the form stated.  $\square$

**Theorem 35.** *The conductor of  $\text{Res}_{\mathbb{Q}}^{K_\beta} E_\beta^t$  is*

$$d_{K_\beta/\mathbb{Q}}^2 \cdot N_{K_\beta/\mathbb{Q}}(\mathfrak{m}) = 2^{8+2\alpha} \cdot 3^8 \cdot 5^{6+\varepsilon} \cdot \prod'_{q|s^2-10st+5t^2} q^4,$$

where the product does not include primes dividing  $2 \cdot 3 \cdot 5$ ;  $\alpha = 0, 4$ , and  $\varepsilon = 0, 2$  according as  $s \not\equiv 0 \pmod{5}$ ,  $s \equiv 0 \pmod{5}$ .

*Proof.* cf. [22, Lemma, p. 178]. We also note that  $K_\beta$  is unramified outside  $\{2, 5\}$  so the product is of the form stated.  $\square$

From here on, we choose  $E$  to be  $E^s$  if  $s \equiv 0 \pmod{5}$  and  $E^t$  if  $s \not\equiv 0 \pmod{5}$ . Thus,  $\varepsilon = 0$  from the theorems above.

In our situation,  $\mathcal{R}_{E_\beta} \cong M_\beta \oplus M_{\beta'} \cong \mathbb{Q}(i) \oplus \mathbb{Q}(i)$ . Let  $M = \mathbb{Q}(i)$ . The conductor of the system of  $M_\pi[G_\mathbb{Q}]$ -modules  $\{\hat{V}_\pi(\text{Res}_{\mathbb{Q}}^{K_\beta} E_\beta)\}$  is one of

$$\begin{aligned} & 2^4 \cdot 3^4 \cdot 5^3 \prod'_{q|s^2-10st+5t^2} q^2, \\ & 2^8 \cdot 3^4 \cdot 5^3 \prod'_{q|s^2-10st+5t^2} q^2, \end{aligned}$$

using Theorem 34 and 35, Lemmas 28 and 29.

We note that the trivial solution  $s = 0, t = 1$  gives rise to the last case and  $E_0 = E_\beta^s$  has complex multiplication by  $\sqrt{-4}$  in this situation. The trivial solution  $s = 1, t = 0$  gives rise to the first case and  $E_1 = E_\beta^t$  has complex multiplication by  $\sqrt{-4}$  in this situation.

For future reference, we will use the notation  $D_q$  and  $I_q$  for a decomposition and inertia group of  $G_\mathbb{Q}$  over the prime  $q$ .

**Theorem 36.** *Let  $f \in S_2(\Gamma_0(N), \psi)$  be a newform.*

- (1) *The conductor of  $\{\hat{\rho}_{f,\pi}\}$  is equal to  $N$ .*
- (2) *Suppose  $q \neq p$  and  $q \parallel N$ .*

*If  $q$  does not divide the conductor of  $\psi$ , then  $\hat{\rho}_{f,\pi}|_{D_q}$  is of the form*

$$\begin{pmatrix} \chi\chi_p & * \\ 0 & \chi \end{pmatrix}.$$

If  $q$  divides the conductor of  $\psi$ , then  $\hat{\rho}_{f,\pi}|_{D_q}$  is of the form

$$\begin{pmatrix} \chi^{-1}\chi_p\psi & 0 \\ 0 & \chi \end{pmatrix}.$$

Here  $\chi$  is the unramified character of  $D_\ell$  which sends  $\text{Fr}_q$  to  $a_q$  and  $\chi_p : G_{\mathbb{Q}} \rightarrow \mathbb{Z}_p^*$  is the  $p$ -th cyclotomic character.

*Proof.* cf. [7, Théorème 2.1], [8, Théorème (A)], [12, Theorem 3.1], [18, (0.1)].  $\square$

The conductor of the system of  $M_\pi[G_{\mathbb{Q}}]$ -modules  $\{\hat{V}_\pi(A_\beta)\}$  is then equal to the level of  $f$ . Similarly, the conductor of the system of  $M_\pi[G_{\mathbb{Q}}]$ -modules  $\{\hat{V}_\pi(A_{\beta'})\}$  is equal to the level of  $f'$ .

We now recall some results about twists of newforms [2]. Let  $f \in S_k(\Gamma_0(N), \psi)$  where  $\psi$  is a character of conductor  $N' | N$ . Let  $\chi$  be a character of conductor  $M$ . Then the twist  $f_\chi$  of  $f$  by  $\chi$  lies in  $S_k(\Gamma_0(\tilde{N}), \psi\chi^2)$  where  $\tilde{N} = \text{lcm}(N, N'M, M^2)$ .

**Theorem 37.** *Let  $q$  be a prime and  $Q$  be the  $q$ -primary factor of the positive integer  $N$ . Write  $N = QM$ . Let  $f$  be a newform in  $S_k(\Gamma_0(N), \psi)$  where the conductor of the  $q$ -primary part  $\psi_q$  of  $\psi$  is equal to  $q^\alpha$  with  $\alpha \geq 0$ . Let  $\chi$  be a character of conductor  $q^\beta$  with  $\beta \geq 1$ . Put  $Q' = \max(Q, q^{\alpha+\beta}, q^{2\beta})$ . Then we have that*

- (1)  $f_\chi$  is of level dividing  $Q'M$ ,
- (2) for each prime  $q' | M$ ,  $f_\chi$  is not of level  $Q'M/q'$ ,
- (3) the exact level of  $f_\chi$  is  $Q'M$  provided
  - (a)  $\max(q^{\alpha+\beta}, q^{2\beta}) < Q$  if  $Q' = Q$  or
  - (b) the conductor of  $\psi_q\chi$  is equal to  $\max(q^\alpha, q^\beta)$  if  $Q' > Q$ .

*Proof.* cf. [2, Theorem 3.1]  $\square$

Since  $f'$  is a twist of  $f$  by the character  $\chi^{-1} = \chi = \left(\frac{5}{\cdot}\right)$  of conductor 5, Theorem 37 shows the level of one of  $f$  or  $f'$  is equal to one of

$$\begin{aligned} 2^2 \cdot 3^2 \cdot 5 \prod'_{q|s^2-10st+5t^2} q &= 180 \prod'_{q|s^2-10st+5t^2} q, \\ 2^4 \cdot 3^2 \cdot 5 \prod'_{q|s^2-10st+5t^2} q &= 720 \prod'_{q|s^2-10st+5t^2} q. \end{aligned}$$

We will for convenience switch the roles of  $f$  and  $f'$  if necessary so the level of  $f$  is as stated above.

For the next two theorems, it is useful to note that  $s - (5 + 2\sqrt{5})t$  and  $s - (5 - 2\sqrt{5})t$  are coprime by Lemma 4.

**Theorem 38.** *The representation  $\phi_{E,p}|_{I_p}$  is finite flat for  $p \neq 2, 3, 5$ .*

*Proof.* This follows from the fact that  $E$  has good or multiplicative bad reduction at primes above  $p$  when  $p \neq 2, 3, 5$ , and in the case of multiplicative bad reduction, the exponent of a prime above  $p$  in the minimal discriminant of  $E$  is divisible by  $p$ . Also,  $p$  is unramified in  $K_\beta$  so that  $I_p \subseteq G_{K_\beta}$ .  $\square$

**Theorem 39.** *The representation  $\phi_{E,p}|_{I_\ell}$  is trivial for  $\ell \neq 2, 3, 5, p$ .*

*Proof.* This follows from the fact that  $E$  has good or multiplicative bad reduction at primes above  $\ell$  when  $\ell \neq 2, 3, 5$ , and in the case of multiplicative bad reduction, the exponent of a prime above  $\ell$  in the minimal discriminant of  $E$  is divisible by  $p$ . Also,  $\ell$  is unramified in  $K_\beta$  so that  $I_\ell \subseteq G_{K_\beta}$ .  $\square$

**Theorem 40.** *Suppose  $p \neq 2, 3$ . The conductor of  $\rho = \rho_{E,\beta,\pi} \cong \rho_{f,\pi}$  is one of 180, 720.*

*Proof.* Suppose  $\ell \neq 2, 3, 5, p$ . Since  $\ell \neq 2, 5$ , we see that  $K_\beta$  is unramified at  $\ell$  and hence  $G_{K_\beta}$  contains  $I_\ell$ . Now, in our case,  $\rho|_{G_{K_\beta}}$  is isomorphic to  $\phi_{E,p}$ . Since  $\phi_{E,p}|_{I_\ell}$  is trivial, we have that  $\rho|_{I_\ell}$  is trivial so  $\rho$  is unramified outside  $\{2, 3, 5, p\}$ .

Suppose  $\ell = 2, 3, 5$ . The representation  $\hat{\phi}_{E,p}|_{I_\ell}$  factors through a finite group of order only divisible by the primes 2, 3. Now, in our case,  $\hat{\rho}|_{G_{K_\beta}}$  is isomorphic to  $\hat{\phi}_{E,p}$ . Hence, the representation  $\hat{\rho}|_{I_\ell}$  also factors through a finite group of order only divisible by the primes 2, 3. It follows that the exponent of  $\ell$  in the conductor of  $\rho$  is the same as in the conductor of  $\hat{\rho}$  as  $p \neq 2, 3$ .  $\square$

**Theorem 41.** *Suppose  $p \neq 2, 3, 5$ . Then the weight of  $\rho_{E,\beta,\pi} \cong \rho_{f,\pi}$  is 2.*

*Proof.* The weight of  $\rho$  is determined by  $\rho|_{I_p}$ . Since  $p \neq 2, 5$ , we see that  $K_\beta$  is unramified at  $p$  and hence  $G_{K_\beta}$  contains  $I_p$ . Now, in our case,  $\rho|_{G_{K_\beta}}$  is isomorphic to  $\phi_{E,p}$ . Since  $\phi_{E,p}|_{I_p}$  is finite flat and its determinant is the

$p$ -th cyclotomic character, we have that the weight of  $\rho$  is 2 [33, Proposition 4].  $\square$

**Theorem 42.** *The character of  $\rho_{E,\beta,\pi} \cong \rho_{f,\pi}$  is  $\epsilon^{-1}$ .*

*Proof.* This follows from Equation (1).  $\square$

**Theorem 43.** *Suppose the representation  $\rho_{E,\beta,\pi}$  is reducible for  $p \neq 2, 3, 5, 7, 13$ . Then  $E$  has potentially good reduction at all primes above  $\ell > 3$ .*

*Proof.* cf. [14, Proposition 3.2].  $\square$

**Corollary 44.** *The representation  $\rho_{E,\beta,\pi}$  is irreducible for  $p \neq 2, 3, 5, 7, 13$ .*

*Proof.* This follows from the fact that a non-trivial proper solution giving rise to  $E$  will be such that  $E$  has a prime of multiplicative bad reduction above a prime not equal to 2, 3, 5 by Corollary 8.  $\square$

**Theorem 45.** *Suppose the representation  $\rho_{E,\beta,\pi}$  has image lying in the normalizer of a split Cartan subgroup for  $p \neq 2, 3, 5, 7, 13$ . Then  $E$  has potentially good reduction at all primes  $\ell > 3$ .*

*Proof.* cf. [14, Proposition 3.4].  $\square$

We note in the context of [14, Proposition 3.2] [14, Proposition 3.4], the reference to a  $\mathbb{Q}$ -curve of degree  $d$  over a quadratic number field  $K$  does not require the isogeny between  $E$  and its conjugate to be also defined over  $K$ . More precisely, we have the following fact.

Let  $X_{0,B}^K(d,p)$ ,  $X_{0,N}^K(d,p)$ ,  $X_{0,N'}^K(d,p)$  be the modular curves with level  $p$  structure corresponding to a Borel subgroup  $B$ , the normalizer of a split Cartan subgroup  $N$ , the normalizer of a non-split Cartan subgroup  $N'$  of  $\mathrm{GL}_2(\mathbb{F}_p)$ , and level  $d$  structure consisting of a cyclic subgroup of order  $d$ , twisted by the quadratic character associated to  $K$  through the action of the Fricke involution  $w_d$ .

**Lemma 46.** *Let  $E$  be a  $\mathbb{Q}$ -curve defined over  $K'$ ,  $K$  be a quadratic number field contained in  $K'$ , and  $d$  a prime number such that*

- (1) *the elliptic curve  $E$  is defined over  $K$ ,*
- (2) *the choices of  $\mu_E(\sigma)$  are constant on  $G_K$  cosets,  $\mu_E(\sigma) = 1$  when  $\sigma \in G_K$ , and  $\deg \mu_E(\sigma) = d$  when  $\sigma \notin G_K$ ,*

(3)  $\mu_E(\sigma)^\sigma \mu_E(\sigma) = \pm d$  whenever  $\sigma \notin G_K$ .

If  $\rho_{E,\beta,\pi}$  has image lying in a Borel subgroup, normalizer of a split Cartan subgroup, normalizer of a non-split Cartan subgroup of  $\overline{\mathbb{F}}_p^\times \mathrm{GL}_2(\mathbb{F}_p)$ , then  $E$  gives rise to a  $\mathbb{Q}$ -rational point on the corresponding modular curve above.

*Proof.* This proof is based on [14, Proposition 2.2]. Note that Ellenberg's  $\mathbb{P}\overline{\rho}_{E,p} : G_{\mathbb{Q}} \rightarrow \mathrm{PGL}_2(\mathbb{F}_p)$  is simply the projectivation of our  $\rho_{E,\beta,\pi} : G_{\mathbb{Q}} \rightarrow \overline{\mathbb{F}}_p^\times \mathrm{GL}_2(\mathbb{F}_p)$  (this does not depend on the choice of  $\beta$ ). The action of  $G_{\mathbb{Q}}$  on  $\mathbb{P}E[p]$  is given by  $x \mapsto \mu_E(\sigma)(^\sigma x)$ . Suppose  $\mathbb{P}\rho_{E,\beta,\pi}$  has image lying in a Borel subgroup. Then we have that  $\mu_E(\sigma)(^\sigma C_p) = C_p$  for some cyclic subgroup  $C_p$  of order  $p$  in  $E[p]$  and all  $\sigma \in G_{\mathbb{Q}}$ . Let  $C_d$  be the cyclic subgroup of order  $d$  in  $E[d]$  defined by  $\mu_E(\tau)(^\tau E[d])$  where  $\tau$  is an element of  $G_{\mathbb{Q}}$  which is non-trivial on  $K$ . This does not depend on the choice of  $\tau$ .

Suppose  $\tau$  is an element of  $G_{\mathbb{Q}}$  which is non-trivial on  $K$ . The kernel of  $\mu_E(\tau)$  is precisely  ${}^\tau C_d$  as  $\mu_E(\tau)({}^\tau C_d) = \mu_E(\tau)^\tau \mu_E(\tau) \left( {}^{\tau^2} E[d] \right) = [\pm d] \left( {}^{\tau^2} E[d] \right) = 0$ . Hence, we see that

$$\begin{aligned} w_d({}^\tau(E, C_d, C_p)) &= w_d({}^\tau E, {}^\tau C_d, {}^\tau C_p) \\ &= (\mu_E(\tau)({}^\tau E), \mu_E(\tau)({}^\tau E[d]), \mu_E(\tau)({}^\tau C_p)) \\ &= (E, C_d, C_p) \end{aligned}$$

so  ${}^\tau(E, C_d, C_p) = w_d(E, C_d, C_p)$  as  $w_d$  is an involution.

Suppose  $\sigma$  is an element of  $G_{\mathbb{Q}}$  which is trivial on  $K$ . In this case, we have that  ${}^\sigma(E, C_d, C_p) = (E, C_d, C_p)$ . For this, note that

$$\begin{aligned} {}^\sigma C_d &= {}^\sigma \mu_E(\tau)({}^\tau E[d]) \\ &= {}^\sigma \mu_E(\tau)({}^{\sigma\tau} E[d]) \\ &= {}^\sigma \mu_E(\tau)({}^\tau E[d]) \\ &= \pm \mu_E(\tau)({}^\tau E[d]) \\ &= C_d \end{aligned}$$

We have that  ${}^\sigma \mu_E(\tau) = \pm \mu_E(\sigma\tau) = \pm \mu_E(\tau)$  because  $E$  does not have complex multiplication and  $G_K$  is normal in  $G_{\mathbb{Q}}$ . Thus,  $(E, C_d, C_p)$  gives rise to a  $\mathbb{Q}$ -rational point on  $X_{0,B}(d, p)$ .

The case when the image of  $\rho_{E,\beta,\pi}$  lies in the normalizer of a Cartan subgroup is similar except now we have the existence of a set of distinct

points  $S_p = \{\alpha_p, \beta_p\}$  of  $\mathbb{P}E[p] \otimes \mathbb{F}_{p^2}$  such that the action of  $\sigma \in G_{\mathbb{Q}}$  by  $x \mapsto \mu_E(\sigma)(\sigma x)$  fixes  $S_p$  as a set.  $\square$

Hence, we may apply Ellenberg's result to  $E/\mathbb{Q}(\sqrt{5})$  as initially given because the hypotheses are satisfied (with  $K' = \mathbb{Q}(\sqrt{5}, \sqrt{2})$ ,  $K = \mathbb{Q}(\sqrt{5})$ ,  $d = 2$ ).

**Corollary 47.** *The representation  $\rho_{E,\beta,\pi}$  does not have image lying in the normalizer of a split Cartan subgroup for  $p \neq 2, 3, 5, 7, 13$ .*

*Proof.* This follows from the fact that a non-trivial proper solution giving rise to  $E$  will be such that  $E$  has a prime of multiplicative bad reduction above a prime not equal to 2, 3, 5 by Corollary 8.  $\square$

It follows from work on the refined Serre's conjectures that  $\rho_{f,\pi} \cong \rho_{g,\pi}$  for a newform  $g \in S_2(\Gamma_0(M), \epsilon^{-1})$  where  $M = 180, 720$ . We have that  ${}^\sigma f = f \otimes \epsilon$  and  ${}^\sigma f' = f' \otimes \epsilon$  where  $\sigma$  is the non-trivial automorphism of  $M = \mathbb{Q}(i)$  by [29, Example 3.7]. We have that  $G_{K_\beta/\mathbb{Q}} \cong (\mathbb{Z}/20\mathbb{Z})^* / \{\pm 1\} = \{\pm 1, \pm 3, \pm 7, \pm 9\}$  and  $\pm 7$  and  $\pm 3$  are each generators of this cyclic group of order 4. Recall we have normalized  $\epsilon(\pm 3) = i$ . From the inner twist property of  $f$  and  $f'$  above (c.f. [29, §3]), we see that  $\epsilon(q) = \pm i$  implies that  $a_q(f) = u + iv$  satisfies  $u \pm v = 0$ . Thus, if  $q \equiv \pm 3 \pmod{20}$ , then we have that  $u + v = 0$  and if  $q \equiv \pm 7 \pmod{20}$ , then we have that  $u - v = 0$ .

Suppose that  $K_g$  is strictly larger than  $\mathbb{Q}(i)$ . Let  $q \neq 2, 3, 5$  be a prime such that  $a_q(g) \notin \mathbb{Q}(i)$ . Assume that  $p \neq q$ . Then we have that

$$\begin{aligned} p & \mid N(a_q(g)^2 - \epsilon^{-1}(q)(q+1)^2) \text{ if } q \mid s^2 - 10st + 5t^2 \\ p & \mid N(a_q(g) - a_q(f)) \text{ if } q \nmid s^2 - 10st + 5t^2. \end{aligned}$$

The former case follows from Theorem 36. In the latter case, we also note that  $a_q(f)$  is restricted by the properties of inner twist above and also by the fact that  $|a_q(f)| < 2\sqrt{q}$ . Hence, for each such prime  $q$ , we obtain that  $p$  is restricted to belong in a finite subset of primes. Taking the intersection of these subsets for different  $q$  further restricts the possibilities for the prime  $p$ .

A computation of  $S_2(\Gamma_0(180), \epsilon^{-1})$  reveals 2 newforms  $g$  such that  $K_g$  strictly contains  $\mathbb{Q}(i)$ . For these, we obtain a bound of  $p \in \{2, 3, 5, 7, 17\}$ .

There are 3 newforms  $g$  such that  $K_g = \mathbb{Q}(i)$  and these all have complex multiplication by  $\mathbb{Q}(\sqrt{-4})$ .

A computation of  $S_2(\Gamma_0(720), \epsilon^{-1})$  reveals 4 newforms  $g$  such that  $K_g$  strictly contains  $\mathbb{Q}(i)$ . For these, we obtain a bound of  $p \in \{2, 3, 5, 7\}$ . There are 3 newforms  $g$  such that  $K_g = \mathbb{Q}(i)$  and these all have complex multiplication by  $\mathbb{Q}(\sqrt{-4})$ .

The computations of modular forms were performed in MAGMA [5] using W. Stein's modular symbols package. The data is posted at

`www.math.sfu.ca/~ichen/x225-data`

for the reader's reference.

**Theorem 48.** *Let  $p > 17$  be a prime such that  $p \equiv 1 \pmod{4}$ . Then the equation  $a^2 + b^{2p} = c^5$  does not have any non-trivial proper solutions.*

*Proof.* If  $p \notin \{2, 3, 5, 7, 13\} \cup \{2, 3, 5, 7, 17\}$ , then we must have that  $\rho_{f,\pi} \cong \rho_{g,\pi}$ , where  $g$  has complex multiplication by  $\mathbb{Q}(\sqrt{-4})$ . If  $p \equiv 1 \pmod{4}$ , then  $\rho_{f,\pi} \cong \rho_{g,\pi}$  would have image lying in the normalizer of a split Cartan subgroup, contradicting Corollary 47.

For the latter fact about the image, we give some details. We are given that  $g$  has complex multiplication by  $F = \mathbb{Q}(\sqrt{-4})$  in the sense that  $a_q(g)\phi(q) = a_q(g)$  for all but finitely many primes  $q$ , where  $\phi$  is the quadratic Dirichlet character associated to  $F$ . By [35],  $A_g$  is isogenous over  $\overline{\mathbb{Q}}$  to the power of an elliptic curve  $C$  with complex multiplication by  $F$ , which we shall take to be  $E_0$  or  $E_1$  defined previously. Hence,  $A_g$  is an abelian variety of  $\text{GL}_2$ -type defined over  $\mathbb{Q}$  attached to  $C$ . We have shown that  $A_g$  is isogenous over  $\mathbb{Q}$  to  $A_\beta$  for some splitting map  $\beta$  for  $c_C(\sigma, \tau)$ . However, we know that  $\det \hat{\rho}_{g,\pi} = \epsilon^{-1}\chi_p$  so the splitting character  $\epsilon_\beta = \epsilon$ . It follows that  $\beta$  is the  $\beta$  defined in Equation (8), up to multiplication by a quadratic Galois character unramified outside  $\{2, 3, 5\}$ . Thus,  $K_\beta$  is unramified outside  $\{2, 3, 5\}$ . We may now take the field of definition of the isogeny between  $A_g$  and  $C^2$  to be  $K_\beta$  by the construction of  $A_\beta$ . Let  $L = K_\beta \cdot F$ . There is an injection of  $M = F \cdot K_g$  into the endomorphism algebra of  $A_g$  defined over  $L$  and  $\hat{V}_p(A_g) \cong M \otimes \mathbb{Q}_p$  as  $G_L$ -modules. Since  $p \equiv 1 \pmod{4}$ ,  $p$  is split in  $M$  and so  $\rho_{g,\pi}|_{G_L}$  has image lying in a split Cartan subgroup of  $\text{GL}_2(k_\pi) = \text{GL}_2(\mathbb{F}_p)$ . This implies that in fact  $\rho_{g,\pi}|_{G_F}$  has image lying in a

split Cartan subgroup of  $\mathrm{GL}_2(\mathbb{F}_p)$ . For we know that  $\rho_{g,\pi}|_{G_F}$  is abelian [28, Proposition (4.4)] so if it does not lie in a split Cartan subgroup of  $\mathrm{GL}_2(\mathbb{F}_p)$ , it must lie in a non-split Cartan subgroup of  $\mathrm{GL}_2(\mathbb{F}_p)$ . Therefore  $\rho_{g,\pi}|_{G_L}$  lies in the center of  $\mathrm{GL}_2(\mathbb{F}_p)$ , implying further that  $\det \rho_{g,\pi}|_{G_L}$  lies in the subgroup of squares of  $\mathbb{F}_p^\times$ . However,  $\det \rho_{g,\pi}|_{G_L} = \bar{\epsilon}^{-1} \bar{\chi}_p$  is surjective to  $\mathbb{F}_p^\times$  since  $L$  does not contain a primitive  $p$ -th root of unity for  $p > 5$ . Finally, as  $[G_{\mathbb{Q}} : G_F] = 2$  it follows that  $\rho_{g,\pi}$  itself has image lying in the normalizer of a split Cartan subgroup of  $\mathrm{GL}_2(\mathbb{F}_p)$  by the classification of subgroups of  $\mathrm{GL}_2(\mathbb{F}_p)$ .  $\square$

## 6. THE INAPPLICABILITY OF MAZUR'S METHOD IN THE NON-SPLIT CARTAN CASE

Let  $d$  be a prime and  $d \neq p$ . Let  $\chi$  be the Dirichlet character associated to a quadratic field  $K$ . The  $\mathbb{Q}$ -curves  $E$  which we associate to a hypothetical solution give rise to a non-cuspidal  $\mathbb{Q}$ -rational points on the modular curve  $X_{0,N'}^K(d,p)$  in the situation when  $\rho_{E,\beta,\pi} \cong \rho_{g,\pi}$  where  $g$  has complex multiplication by  $F$ ,  $p$  is inert in  $F$ , and where  $K = \mathbb{Q}(\sqrt{5})$ .

Let  $X_{0,N'}(d,p)$  be the modular curve with level  $p$  structure corresponding to the normalizer of a non-split Cartan subgroup  $N'$  of  $\mathrm{GL}_2(\mathbb{F}_p)$  and level  $d$  structure consisting of a cyclic subgroup of order  $d$ . Let  $J_{0,N'}(d,p)$  be the jacobian of  $X_{0,N'}(d,p)$  and  $J_{0,N'}^K(d,p)$  be the jacobian of  $X_{0,N'}^K(d,p)$ .

From the arguments in [15], there is an isogeny

$$(22) \quad \pi : J_{0,N'}(d,p) \rightarrow \prod_{[f] \in N_2^+(\Gamma_0(p^2))} A_{[f]} \prod_{[f] \in N_2^+(\Gamma_0(p^2))} A_{[f]} \prod_{[f] \in N_2^{\mp,+}(\Gamma_0(dp^2))} A_{[f]} \prod_{[f] \in N_2^{-,+}(\Gamma_0(dp^2))} A_{[f]},$$

where  $A_{[f]}$  is the abelian variety attached to  $[f]$ , the Galois conjugacy class of  $f$ . Here  $N_2^+(\Gamma_0(p^2))$  is the set of Galois conjugacy classes of newforms of weight 2 and level  $p^2$  such that  $w_{p^2} f = f$ ;  $N_2^{\mp,+}(\Gamma_0(dp^2))$  is similarly defined except  $w_d f = \mp f$ ,  $w_{p^2} f = f$ , and the level is  $dp^2$ . Note that the Atkin-Lehner involutions commute with the action of Galois on the coefficients of modular forms so  $N_2^+(\Gamma_0(p^2))$  and  $N_2^{\mp,+}(\Gamma_0(dp^2))$  are well-defined.

Let

$$\begin{aligned}\pi_1 : J_{0,N'}(d,p) &\rightarrow \prod_{[f] \in N_2^+(\Gamma_0(p^2))} A_{[f]} \\ \pi_2 : J_{0,N'}(d,p) &\rightarrow \prod_{[f] \in N_2^+(\Gamma_0(p^2))} A_{[f]} \\ \pi_3 : J_{0,N'}(d,p) &\rightarrow \prod_{[f] \in N_2^{+,+}(\Gamma_0(dp^2))} A_{[f]} \\ \pi_4 : J_{0,N'}(d,p) &\rightarrow \prod_{[f] \in N_2^{-,+}(\Gamma_0(dp^2))} A_{[f]}\end{aligned}$$

be the homomorphisms obtained by composing the projection to the given group of factors with  $\pi$ . Then we have that  $\pi_i \circ w_d = \pi_i$  for  $i = 1, 3$  and  $\pi_i \circ w_d = -\pi_i$  for  $i = 2, 4$  [15].

The isogeny arises from the fact that  $J_{0,N'}(d,p)$  is isogenous over  $\mathbb{Q}$  to the  $p$ -new quotient of  $J_0(dp^2)/w_p$  (cf. [13]) which decomposes up to isogeny over  $\mathbb{Q}$  into the above product (cf. [29]).

The twist by  $\chi$  is obtained through the action of  $w_d$  on  $X_{0,N'}(d,p)$ . Hence,  $J_{0,N'}^K(d,p)$  is isogenous over  $\mathbb{Q}$  to

$$\prod_{[f] \in N_2^+(\Gamma_0(p^2))} A_{[f]} \prod_{[f] \in N_2^+(\Gamma_0(p^2))} A_{[f_\chi]} \prod_{[f] \in N_2^{+,+}(\Gamma_0(dp^2))} A_{[f]} \prod_{[f] \in N_2^{-,+}(\Gamma_0(dp^2))} A_{[f_\chi]}$$

where

$$f_\chi = \sum_n \chi(n) a_n(f) q^n.$$

Let  $\lambda_Q(f)$  be the pseudo-eigenvalue [2] for a newform  $f \in S_k(\Gamma_0(N), \epsilon)$  with respect to the Atkin-Lehner involution  $w_Q$  where  $Q$  is a  $q$ -primary factor of  $N$ .

**Theorem 49.** *Let  $f$  be a newform in  $S_k(\Gamma_0(N), \epsilon)$  and  $\chi$  a character of conductor  $m$  prime to  $N$ . Then  $f_\chi$  is a newform in  $S_k(\Gamma_0(Nm^2), \epsilon\chi^2)$  and*

$$\lambda_{Nm^2}(f_\chi) = \epsilon(m)\chi(-N) \frac{g(\chi)}{g(\bar{\chi})} \lambda_N(f).$$

*Proof.* cf. the statement in [2, p. 228] based on a Theorem of Weil [39] stated in [21, Theorem 6].  $\square$

Suppose  $K$  is real,  $d$  is inert in  $K$ , and the conductor of  $\chi$  is equal to  $m$  which is prime to  $N$ . In our situation,  $K = \mathbb{Q}(\sqrt{5})$ ,  $\chi = \left(\frac{5}{\cdot}\right)$ ,  $m = 5$ ,  $d = 2$ , and  $N = dp^2$ . We then have that  $\chi(-p^2) = 1$  and  $\chi(-dp^2) = -1$ . For  $[f] \in N_2^+(\Gamma_0(p^2))$ ,  $\lambda_{p^2 m^2}(f_\chi) = \chi(-p^2)\lambda_{p^2}(f) = 1$  by Theorem 49. For  $[f] \in N_2^{-,+}(\Gamma_0(dp^2))$ ,  $\lambda_{dp^2 m^2}(f_\chi) = \chi(-dp^2)\lambda_{dp^2}(f) = 1$  by Theorem 49. Thus, for  $[f] \in N_2^+(\Gamma_0(p^2))$  and  $[f] \in N_2^{-,+}(\Gamma_0(dp^2))$ ,  $L([f_\chi], s)$  has sign  $-1$  in its functional equation because the sign for  $L(f_\chi, s)$  is  $-\lambda_{Nm^2}(f_\chi)$  (cf. [23, Theorem 4.3.6] in case  $k = 2$ ).

This implies every non-zero quotient of  $J_{0,N'}^K(d, p)$  has even order of vanishing at  $s = 1$  and hence positive rank over  $\mathbb{Q}$ , assuming the Birch-Swinnerton-Dyer conjectures for abelian varieties. Hence, Mazur's method is inapplicable to the modular curves  $X_{0,N'}^K(d, p)$  in our situation.

## 7. CONCLUSION

It would be interesting to see if a few more cases of the generalized Fermat equation can be handled using  $\mathbb{Q}$ -curves. Indeed, it would be worthwhile to have a more conceptual and precise understanding as to which exponents we can expect to resolve using elliptic curves and what properties these elliptic curves should have (thanks to C. Skinner for asking this question and pointing out the references below). In the case of prime exponents, this was analyzed in [16], and in [11] one has a conceptual starting point to answer this question.

In order to construct Frey curves for use in the modular method, a natural class of objects to consider are genus zero congruence subgroups of  $\mathrm{SL}_2(\mathbb{Z})$  with exactly three special points (i.e. elliptic points or cusps). From [10], the following is the list of such modular curves,

- $X(1), (2, 3, \infty)$ ,
- $X_0(2), (2, \infty, \infty)$ ,
- $X_0(3), (3, \infty, \infty)$ ,
- $X(2), (\infty, \infty, \infty)$ ,
- $X_0(4), (\infty, \infty, \infty)$ ,

where we list the orders of the stabilizers in  $\mathrm{PSL}_2(\mathbb{Z})$  of the three special points.

Let  $l_1(u, v), l_2(u, v), l_3(u, v)$  be three homogeneous linear polynomials in  $\overline{\mathbb{Q}}[u, v]$ . It is possible to construct a Frey curve from  $X_0(2)$  which can potentially solve the system of equations  $l_1(u, v) = c^2, l_2(u, v) = a^p, l_3(u, v) = b^p$ . For example, if  $l_1(u, v) = u + v$  and  $l_2(u) = u$  and  $l_3(v) = v$ , then the resulting Frey curve potentially solves  $a^p + b^p = c^2$ . The construction proceeds as follows. The  $j$ -invariant is a rational function of a uniformizer  $t$  for  $X_0(2)$ , and we have that

$$j = (t + 256)^3/t^2$$

$$j - 1728 = \frac{(t + 64)(t - 512)^2}{t^2}$$

for one such choice of uniformizer  $t$ . Let  $s_1, s_2, s_3$  be the roots corresponding to  $l_1, l_2, l_3$ . Let  $t$  be a Möbius transformation of  $s$  such that  $s = s_1, s_2, s_3$  are sent to  $t = -64, 0, \infty$ . Writing  $j$  as a rational function of  $s$ , and then taking  $E$  to be an elliptic curve with  $j$ -invariant equal to  $j$  gives the desired Frey curve after setting  $s = u/v$ . It is usually beneficial to twist the resulting Frey curve  $E$  so that its conductor is smaller than initially given.

An additional constraint on  $E$  is that it should have attached Galois representations which we are able to handle through modularity. In the example given above,  $E$  would be defined over  $\mathbb{Q}$  and so we can attach to  $E$  the usual 2-dimensional  $\ell$ -adic representations of  $G_{\mathbb{Q}}$ .

Another situation is when  $l_1(u, v) \in \mathbb{Z}[u, v]$  and  $l_2(u, v)l_3(u, v)$  is irreducible in  $\mathbb{Z}[u, v]$ . In this case,  $E$  is a  $\mathbb{Q}$ -curve defined over some number field containing the associated roots of  $l_2(u, v)l_3(u, v)$ , and it is possible to attach 2-dimensional  $\ell$ -adic representations of  $G_{\mathbb{Q}}$  to  $E$ . For example, when  $l_1(u, v) = u$  or  $v$ , and  $l_2(u, v)l_3(u, v) = u^2 - 10uv + 5v^2$ , the above construction gives the  $\mathbb{Q}$ -curves  $E^s$  and  $E^t$  used in this paper.

## 8. ACKNOWLEDGEMENTS

I would like to thank M. Bennett, J. Ellenberg, S. Siksek, C. Skinner for many useful discussions and suggestions. I would like to also thank the Department of Mathematical Sciences at the University of Copenhagen, the Banff International Research Station, and the Lorentz Center for their hospitality and support during the author's visits there in 2006–2007.

## REFERENCES

- [1] *Groupes de monodromie en géométrie algébrique. I.* Springer-Verlag, Berlin, 1972. Séminaire de Géométrie Algébrique du Bois-Marie 1967–1969 (SGA 7 I), Dirigé par A. Grothendieck. Avec la collaboration de M. Raynaud et D. S. Rim, Lecture Notes in Mathematics, Vol. 288.
- [2] A.O.L. Atkin and W.-C. Li. Twists of newforms and pseudo-eigenvalues of W-operators. *Inventiones Mathematicae*, 48:221–243, 1978.
- [3] M. Bennett. Diophantine equations after Wiles. CNTA VIII, Ribenboim Prize Lecture, 23 June 2004.
- [4] M. Bennett and C. Skinner. Ternary diophantine equations via galois representations and modular forms. *Canadian Journal of Mathematics*, 56(1):23–54, 2004.
- [5] W. Bosma, J. Cannon, and C. Playoust. The Magma algebra system. I. The user language. Computational algebra and number theory (London, 1993). *J. Symbolic Comput.*, 24(3-4):235–265, 1997.
- [6] J. Buhler and B. Gross. Arithmetic on elliptic curves with complex multiplication II. *Invent. Math.*, 79:11–29, 1985.
- [7] H. Carayol. Sur les représentations attachés aux forms modulaire de Hilbert. *C. R. Acad. Sci. Paris Série I*, 196:629, 1983.
- [8] H. Carayol. Sur les représentations  $p$ -adiques associées aux forms modulaire de Hilbert. *Ann. Sci. Ecole Norm. Sup.*, 19:409–468, 1986.
- [9] I. Chen. On the equation  $s^2 + y^{2p} = \alpha^3$ . *Math. Comp.*, 77(262):1223–1227, 2007.
- [10] C. Cummins and S. Pauli. Congruence subgroups of  $\mathrm{PSL}_2(\mathbb{Z})$  of genus less than or equal to 24. *Experiment. Math.*, 12(2):243–255, 2003.
- [11] H. Darmon. Rigid local systems, Hilbert modular forms, and Fermat’s Last Theorem. *Duke Math Journal*, 102:413–449, 2000.
- [12] H. Darmon, F. Diamond, and Taylor R. Fermat’s Last Theorem. In *Elliptic curves, modular forms & Fermat’s Last Theorem (Hong Kong, 1993)*, pages 2–140. International Press, 1997.
- [13] H. Darmon and L. Merel. Winding quotients and some variants of Fermat’s Last Theorem. *Journal für die Reine und Angewandte Mathematik*, 490:81–100, 1997.
- [14] J. Ellenberg. Galois representations attached to  $\mathbb{Q}$ -curves and the generalized Fermat equation  $A^4 + B^2 = C^p$ . *American Journal of Mathematics*, 126:763–787, 2004.
- [15] J. Ellenberg and C. Skinner. On the modularity of  $\mathbb{Q}$ -curves. *Duke Math. J.*, 109(1):97–122, 2001.
- [16] A. Granville and H. Darmon. On the equations  $x^p + y^q = z^r$  and  $z^m = f(x, y)$ . *Bulletin of the London Math. Society.*, 27(129):513–544, 1995.
- [17] B. Gross. *Arithmetic on Elliptic Curves with Complex Multiplication*. Number 776 in Lecture Notes in Mathematics. Springer-Verlag, 1980.
- [18] B.H. Gross. A tameness criterion for Galois representations associated to modular forms (mod  $p$ ). *Duke Math. J.*, 61(2):445–517, 1990.
- [19] A. Kraus. Sur l’équation  $a^3 + b^3 = c^p$ . *Experiment. Math.*, 7:1–13, 1998.
- [20] A. Kraus. On the equation  $x^p + y^q = z^r$ : A survey. *The Ramanujan Journal*, 3:315–333, 1999.
- [21] W. Li. Newforms and Functional Equations. *Math. Ann.*, 212:285–315, 1975.
- [22] J. Milne. On the arithmetic of abelian varieties. *Inventiones Math.*, 17:177–190, 1972.
- [23] T. Miyake. *Modular Forms*. Springer-Verlag, 1989.

- [24] H. Montgomery and P. Weinberger. Notes on small class numbers. *Acta Arith.*, 24:529–542, 1973/74.
- [25] A.P. Ogg. Elliptic curves and wild ramification. *American Journal of Mathematics*, 89:1–21, 1967.
- [26] I. Papadopoulos. Sur la classification de Néron des courbes elliptiques en caractéristique résiduelle 2 et 3. *Journal of Number Theory*, 44:119–152, 1993.
- [27] J. Quer.  $\mathbb{Q}$ -curves and abelian varieties of  $GL_2$ -type. *Proc. London Math. Soc.*, 81(3):285–317, 2000.
- [28] K. Ribet. Galois representations attached to eigenforms with nebentypus. In *Modular Functions of One Variable V (Bonn, 1976)*, number 601 in Lecture Notes in Mathematics, pages 17–51. Springer-Verlag, 1972.
- [29] K. Ribet. Twists of modular forms and endomorphisms of abelian varieties. *Math. Ann.*, 253:43–62, 1980.
- [30] K. Ribet. Abelian varieties over  $\mathbb{Q}$  and modular forms. In *Algebra and Topology 1992*, Korea Adv. Inst. Sci. Tech., pages 53–79, 1992.
- [31] J.-P. Serre. *Corps locaux*. Number VIII in Publications de l'Université de Nancago. Hermann, Paris, deuxième édition, 1968.
- [32] J.-P. Serre. Modular forms of weight one and galois representations. In Frölich A., editor, *Algebraic Number Fields*, pages 193–268. Academic Press, 1977.
- [33] J.-P. Serre. Sur les représentations modulaires de degré 2 de  $\text{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})$ . *Duke Mathematical Journal*, 54(1):179–230, 1987.
- [34] J.-P. Serre and J. Tate. Good reduction of abelian varieties. *Annals of Mathematics*, 88:492–517, 1968.
- [35] G. Shimura. On elliptic curves with complex multiplication as factors of the jacobians of modular function fields. *Nagoya Math. J.*, 43:199–208, 1971.
- [36] J.H. Silverman. *Advanced Topics in the Arithmetic of Elliptic Curves*. Springer-Verlag, 1994.
- [37] H. Stark. On complex quadratic fields with class-number two. *Math. Comp.*, 29:289–302, 1975.
- [38] M.-F. Vigneras. *Arithmétique de algèbres de quaternions*. Number 800 in Lecture notes in mathematics. Springer-Verlag, 1980.
- [39] A. Weil. Über die Bestimmung Dirihletscher Reihen durch Funktionalgleichungen. *Math. Ann.*, 168:149–156, 1967.

DEPARTMENT OF MATHEMATICS, SIMON FRASER UNIVERSITY, BURNABY, BRITISH COLUMBIA, CANADA V5A 1S6

*E-mail address:* `ichen@math.sfu.ca`