ACTA ARITHMETICA
143.4 (2010)

On the equation $a^2 + b^{2p} = c^5$

by

Imin Chen (Burnaby)

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 GL_2-type attached to them. We use the results developed in [14], where the use of $\mathbb{Q}$-curves for studying cases of the generalized Fermat equation was first introduced. To deal with $\mathbb{Q}$-curves defined over quartic extensions of $\mathbb{Q}$, it is also necessary to use some other 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 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 that conjecturally these jacobians do not have any non-zero quotients over $\mathbb{Q}$ with rank 0 (see Section 6). The situation still does not change if the N' level structure on mod p torsion points is replaced by a twisted C' level structure.

2010 *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.

DOI: 10.4064/aa143-4-3

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. ∎

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 $(v,v^4-10v^2u^2+5u^4)\mid 5$. Setting y to be a pth 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

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

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

For the equation $a^{2p}+b^{2p}=c^5$, one can set both x and y to be pth powers 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 pth power, we can complete the square in the following way to obtain a solution to an equation of the form $Aa'^n+Bb'^n=Cc'^2$:

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

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 pth 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 the cases of 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, which gives 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 $5^j \gamma^p = s^2 - 10st + 5t^2 \equiv -4s^2 \pmod 8$. This is a contradiction if p is an odd prime. ■

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 $\mathbb{F}_3[s, t]$. ■

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 MAGMA [5] to determine the integer solutions to the quartic equation $5Y^2 = 4X^4 \pm 1$. ■

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 MAGMA to determine the integer solutions to the quartic equation $5Y^2 = 4X^4 \pm 5$. ■

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, 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. ∎

2. $\mathbb{Q}$-curves and abelian varieties of 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 $\mu_C(\sigma) : {}^{\sigma}C \to C$ 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 following. The exposition below follows closely the papers cited 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 $c_C(\sigma,\tau) = \mu_C(\sigma){}^{\sigma}\mu_C(\tau)\mu_C(\sigma\tau)^{-1} \in (\mathrm{Hom}_K(C,C) \otimes_{\mathbb{Z}} \mathbb{Q})^* = \mathbb{Q}^*$, where $\mu_C^{-1} := (1/\deg \mu_C)\mu_C'$ and μ_C' is the dual of μ_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 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, so that there is a continuous map $\beta : G_{\mathbb{Q}} \to \overline{\mathbb{Q}}^*$ 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 β 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 $\mathrm{End}_{\mathbb{Q}} A$ 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 λ_σ 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 on the function μ_C. Consider the restriction of scalars $\mathrm{Res}_{\mathbb{Q}}^{K} C$, for which we recall its defining functorial property that $\mathrm{Hom}(S, \mathrm{Res}_{\mathbb{Q}}^{K} C) \leftrightarrow \mathrm{Hom}(S \otimes K, C)$. There is a natural isomorphism

$$\mathcal{R}_C \to \mathrm{End}_{\mathbb{Q}} \mathrm{Res}_{\mathbb{Q}}^{K} C$$

which sends λ_σ to the endomorphism of $\mathrm{Res}_{\mathbb{Q}}^{K} C$ defined by $P \mapsto {}^{\tau}\mu_C(\sigma)(P)$ on ${}^{\sigma\tau}C$.

Given a splitting map β for C, *we now enlarge* K *if necessary* so that β factors through $G_{K/\mathbb{Q}}$. The map given by $\lambda_\sigma \mapsto \beta(\sigma)$ gives a surjective homomorphism $\mathcal{R}_C \to M_\beta = \mathbb{Q}(\beta(\sigma))$. As $\mathcal{R}_C$ is a semisimple $\mathbb{Q}$-algebra, there is a projection from $\mathcal{R}_C$ onto the isomorphic copy of M_β in $\mathcal{R}_C$. Let A_β 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_β above which is useful in practice to minimize the degree of the extension K required (recall K needs to be large enough so that both $c_C(\sigma,\tau)$ and $\beta(\sigma)$ factor through $G_{K/\mathbb{Q}}$). Suppose that

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

as 2-cocycles, where $\epsilon(\sigma,\tau)$ is the 2-coboundary obtained from a 1-cocycle ${}^{\sigma}\sqrt{\gamma}/\sqrt{\gamma}$ 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_γ 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_γ allows us to only require that K be large enough so that $\beta(\sigma)$ factors through $G_{K/\mathbb{Q}}$.

Recall that an abelian variety defined over $\mathbb{Q}$ is *of* GL_2*-type* if its 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 GL_2-type is *attached to a* $\mathbb{Q}$*-curve* C if C is its quotient over $\overline{\mathbb{Q}}$.

THEOREM 9 (cf. [30, Theorem 6.1]). *The abelian variety A_β is an abelian variety defined over $\mathbb{Q}$ of GL_2-type attached to C, with endomorphism algebra isomorphic to M_β.* ∎

PROPOSITION 10. *If A is an abelian variety defined over $\mathbb{Q}$ of GL_2-type attached to a $\mathbb{Q}$-curve C, then A is isogenous over $\mathbb{Q}$ to some A_β where β is a splitting map for C.*

Proof. If C is a quotient of A defined over K, then there is a non-zero homomorphism $A \to \mathrm{Res}_{\mathbb{Q}}^K C$ 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 semisimple $\mathbb{Q}$-algebra, there is a projection $\mathcal{R}_C \to \mathrm{End}_{\mathbb{Q}} A$ given by $\lambda_\sigma \mapsto \beta(\sigma)$ say. We now see that β is a splitting map for C, and that A_β is isogenous over $\mathbb{Q}$ to A. ∎

PROPOSITION 11 (cf. [27, Proposition 5.1, Lemma 5.3]). *Suppose that $\mathcal{R}_C$ is a product of fields. Then $\mathrm{Res}_{\mathbb{Q}}^K C$ is isogenous over $\mathbb{Q}$ to a product of pairwise non-isogenous abelian varieties defined over $\mathbb{Q}$ of GL_2-type, each of the form A_β where β is a splitting map for C. Furthermore, A_{β_1} is isogenous over $\mathbb{Q}$ to A_{β_2} if and only if $\beta_2 = {}^{\sigma}\beta_1$ for some $\sigma \in G_{\mathbb{Q}}$.* ∎

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. *$\hat{V}_p(\mathrm{Res}_{\mathbb{Q}}^K C) \cong \mathcal{R}_C \otimes \hat{V}_p(C)$ 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 C is a $\mathbb{Q}$-curve defined over K and let $A = \mathrm{Res}_{\mathbb{Q}}^{K} C$. 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 λ_g taking the factor C_σ to $C_{g\sigma}$ via multiplication by $c_C(g,\sigma)$. Let $\iota : T_K \to B_K$ be the map which takes the factor C_σ to ${}^{\sigma^{-1}}C$ via the map ${}^{\sigma^{-1}}\mu_C(\sigma)$. Then ι is an $\mathcal{R}_C[G_K]$-equivariant isomorphism. By the above-defined action of $\mathcal{R}_C$ on T_K, we have $\hat{V}_p(T_K) \cong \mathcal{R}_C \otimes \hat{V}_p(C)$ 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

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

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 π of M_β above p, we get a representation $\hat{\rho}_{C,\beta,\pi} : G_{\mathbb{Q}} \to \mathrm{GL}_2(M_{\beta,\pi})$. 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

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

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

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

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

Then ϵ_β is a character and

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

where $\chi_p : G_{\mathbb{Q}} \to \mathbb{Z}_p^*$ is the pth cyclotomic character.

Given two splitting maps β, β' for C, there is a character $\chi : G_{\mathbb{Q}} \to \overline{\mathbb{Q}}^*$ such that $\beta' = \chi\beta$. Conversely, if β is a splitting map, then $\beta' = \chi\beta$ is a splitting map for any character $\chi : G_{\mathbb{Q}} \to \overline{\mathbb{Q}}^*$. 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_β.

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 GL_2-type attached to C. This is because $J_1(N)$ decomposes into a product of A_f's up to isogeny over $\mathbb{Q}$ [29]. By Proposition 10, A_f is isogenous to A_β for some splitting map β, and hence for some splitting map β for C we have $\rho_{C,\beta,\pi} \cong \rho_{f,\pi}$ 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 β we have $\rho_{C,\beta,\pi} \cong \rho_{f,\pi}$ 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_β 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

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

Then

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

and

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

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

The $\mathbb{Q}$-curve E^s satisfies 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 pth 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

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

Then

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

and

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

The $\mathbb{Q}$-curve E^t satisfies 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 pth power up to S-units for a finite set of primes S, using the modular method.

The superscripts 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. ∎

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. ∎

The elliptic curves with complex multiplication by an imaginary quadratic order $\mathcal{O}$ of class number 2 are listed below (cf. [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	$-98415459270397440000000 \pm 10432017818647326720000\sqrt{89}$
-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 -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 $s/t \in \mathbb{Q}$. ■

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 -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 $s/t \in \mathbb{Q}$. ■

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. ■

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. ■

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 Corollaries 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 $\hat{\rho}_{E,\beta,\pi} : G_{\mathbb{Q}} \to \mathrm{GL}_2(M_{\beta,\pi})$ attached to the $\mathbb{Q}$-curve E. However, the construction depends on the choice of a splitting map $\beta : G_{\mathbb{Q}} \to \overline{\mathbb{Q}}^*$ 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 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 ${}^{\sigma_5}E \to E$ 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 ω_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

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

which is derived from the short exact sequence

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

Explicitly,

$$\alpha_{E^s}(\sigma_1) = 1, \quad \alpha_{E^s}(\sigma_5) = \frac{1 + \sqrt{5}}{\sqrt{2}},$$
$$\alpha_{E^t}(\sigma_1) = 1, \quad \alpha_{E^t}(\sigma_5) = \sqrt{2}.$$

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

$$c_E(\sigma_2, \sigma_2) = 1, \quad c_E(\sigma_{10}, \sigma_{10}) = 2, \quad c_E(\sigma_2, \sigma_{10}) = -c_E(\sigma_{10}, \sigma_2).$$

It follows that $\mathcal{R}_E \cong M_2(\mathbb{Q})$ and hence $\mathrm{Res}_{\mathbb{Q}}^{\mathbb{Q}(\sqrt{5},\sqrt{2})} E$ is isogenous over $\mathbb{Q}$ to $B \times B$ where B is an abelian surface defined over $\mathbb{Q}$ with $\mathrm{End}_{\mathbb{Q}} B = \mathbb{Q}$. 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 $\mathrm{Res}_{\mathbb{Q}}^{\mathbb{Q}(\sqrt{5},\sqrt{2})} E$ up to isogeny over $\mathbb{Q}$ does not include any abelian varieties of GL_2-type.

Proposition 19 (cf. [27, p. 294]). *The map on cocycles given by*

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

induces an isomorphism

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

where P is the group of positive rational numbers. ∎

We call $c^{\pm}(\sigma,\tau) = \operatorname{sgn} c(\sigma,\tau)$ 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], $\{a_1\} = \{5\}$ and $\{d_1\} = \{2\}$ are dual bases with respect to $d(\sigma)$. The conclusion then follows from [27, Theorem 3.1]. ∎

Let $\epsilon : G_{\mathbb{Q}} \to \overline{\mathbb{Q}}^*$ 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 (cf. [27, Theorem 4.2]). *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 $H^2(G_{\mathbb{Q}}, \{\pm 1\})$.*

Proposition 22 (cf. [27, p. 302]). *$\theta_\epsilon(\sigma,\tau) = c_E^{\pm}(\sigma,\tau)$ 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.*

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 $\mathbb{Q}_p$, that is, quaternion algebras over $\mathbb{Q}_p$ (cf. [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 (cf. [38, Theorem 1.1]). ∎

Proposition 24 (cf. [27, p. 302]). *$\theta_\epsilon(\sigma,\tau)_p = \epsilon_p(-1)$ as classes in $H^2(G_{\mathbb{Q}_p}, \{\pm 1\}) \cong \{\pm 1\}$.*

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

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

where $d(\sigma) = \deg \mu_E(\sigma)$, $\epsilon = \epsilon_4\epsilon_5$, ϵ_4 is the non-trivial character of $(\mathbb{Z}/4\mathbb{Z})^*$, and ϵ_5 is a non-trivial character of $(\mathbb{Z}/5\mathbb{Z})^*$. For this choice of β, we have

$\epsilon_\beta = \epsilon$ and $M_\beta = \mathbb{Q}(i)$. The character ϵ has kernel $\{\pm 1\}$, regarded as a character of $(\mathbb{Z}/20\mathbb{Z})^\times$. To fix choices, 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_β defined over a number field K_β 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 $\alpha_1(\sigma) = \alpha_E(\sigma)^\sigma\sqrt{\gamma_1}/\sqrt{\gamma_1}$, where $\gamma_1 = (5+\sqrt{5})/2$. Then

$$\alpha_1(\sigma_1) = 1, \qquad \alpha_1(\sigma_5) = \sqrt{2}.$$

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 ± 1).

We wish to find a γ_2 such that

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

satisfies

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

Let $K_\beta = \mathbb{Q}(z)$ where $z = \sqrt{(5+\sqrt{5})/2}$ 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_β 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 $g^2/2 = {}^{\sigma_5^+}\gamma_2/\gamma_2$ is a necessary constraint on g using (9). As an initial guess, suppose that $g^2/2 = u$ is a unit in K_β. This unit $u = 2 - z$ can be obtained by noting $(2) = (g^2)$ in K_β. Since $N_{K_\beta/\mathbb{Q}}(u) = 1$, by Hilbert 90, there is a $\gamma_2 \in K_\beta$ such that ${}^\sigma\gamma_2/\gamma_2 = u$, where $\sigma = \sigma_5^+$. This γ_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 $\gamma_2 = 1/\gamma_2' = z^3 + z^2 - 2z$.

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

$$\gamma = z^2(z^3 + z^2 - 2z) = 3z^3 + 5z^2 - 5z - 5 = z^3/u_3,$$

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:

$$\frac{{}^{\sigma_5^+}\gamma}{\gamma} = \frac{g^2}{2}, \qquad \frac{{}^{\sigma_5^-}\gamma}{\gamma} = \frac{g^2}{2}\frac{1}{u_4^2},$$
$$\frac{{}^{\sigma_1^+}\gamma}{\gamma} = 1, \qquad \frac{{}^{\sigma_1^-}\gamma}{\gamma} = u_3^2,$$

which show that $\alpha_2(\sigma)$ has values in K_β.

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

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

Then

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

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

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 the consideration of how twisting affects the $\alpha_E(\sigma)$ [27, p. 291], we have

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

where $\xi(\sigma) \in \{\pm 1\}$. Replacing the choices of $\mu_{E_\beta}(\sigma)$ for E_β (which result from E_β being a twist of E) by $\mu_{E_\beta}(\sigma)\xi(\sigma)$, we get a choice of $\mu_{E_\beta}(\sigma)$'s for E_β which are locally constant on G_{K_β} and such that the values $\alpha_2(\sigma)$ lie in K_β. Hence, if we use E_β instead of E, then E_β is a $\mathbb{Q}$-curve defined over K_β and we have

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

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 GL_2-type with endomorphism algebra $\mathbb{Q}(i)$. Here, $\beta' = \chi\cdot\beta$ is a splitting map such that $\epsilon_{\beta'} = \epsilon$ and $\chi = \left(\frac{5}{\cdot}\right)$ is the quadratic character attached to $\mathbb{Q}(\sqrt{5})$.

A similar calculation can be made for $E = E^t$ with exactly the same β 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*
$$c_E^{\pm}(\sigma,\tau) = \operatorname{sgn}\mu_E(\sigma)\,{}^{\sigma}\mu_E(\tau)\mu_E(\sigma\tau)^{-1} \in H^2(G_{\mathbb{Q}},\{\pm 1\})$$
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 (4), (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 $G_{\mathbb{Q}_3}$. ∎

THEOREM 26. *The abelian varieties A_β 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. ∎

The abelian varieties A_β 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_β and $A_{\beta'}$ respectively.

THEOREM 27. *$A_{\beta'}$ is isogenous over $\mathbb{Q}$ to a twist of A_β 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_β and $A_{\beta'}$ which is given by
$$x \otimes y \mapsto x \cdot \beta(\sigma)^{-1} \otimes \mu_E(\tau)(\tau(y)),$$
$$x \otimes y \mapsto x \cdot \beta'(\sigma)^{-1} \otimes \mu_E(\tau)(\tau(y)).$$
Since $\beta' = \chi\cdot\beta$, we see that $\hat{\rho}_{A,\beta',\pi}(\sigma) = \epsilon^{-1}(\sigma)\hat{\rho}_{A,\beta,\pi}(\sigma)$, where π 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 $\rho_{E,\beta,\pi} : G_{\mathbb{Q}} \to \overline{\mathbb{F}}_p^{*}\mathrm{GL}_2(\mathbb{F}_p)$ 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_β.

The discriminant of K_β is given by $d_{K_\beta/\mathbb{Q}} = 2^4 \cdot 5^3 = 2000$. The prime factorizations of (2), (3), and (5) in K_β are given as follows:
$$(2) = \mathfrak{q}_2^2, \quad (3) = \mathfrak{q}_3, \quad (5) = \mathfrak{q}_5^4.$$

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 π of M, let $\hat{V}_\pi$ be a free M_π-module of rank n with a continuous M_π-linear action of G_K. A collection $\{\hat{V}_\pi\}$ of such $\hat{V}_\pi$'s where π 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 π-adic Tate module $\hat{V}_\pi(A)$ of A is isomorphic to M_π^d and can be obtained as $\hat{V}_\pi(A) = \hat{V}_p(A) \otimes_{M_p} M_\pi$, where M_π is regarded as an M_p-module under the projection $M_p \to M_\pi$.

For each prime π of M, there exists an M_π-basis for $\hat{V}_\pi$ such that the $\mathcal{O}_\pi$-module Λ_π 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 $\rho_\pi : G_K \to \mathrm{GL}(\hat{V}_\pi)$ 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

- there is an open subgroup of I_K whose action on $\hat{V}_\pi$ is unipotent,
- the character of $\hat{V}_\pi$ as an $M_\pi[G_K]$-module has values in M which are independent of π.

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

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

for any $\pi \nmid \ell$. This quantity is a non-negative integer which is independent of π from arguments found in Ogg [25] and 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 λ runs through all finite primes λ of K, and e_λ 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 λ.

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 the conductor exponent. ∎

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 π. Fix a prime $\lambda \,|\, \ell$ 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 $\pi \,|\, p$ and $p \neq \ell$. Since we are free to choose $p \neq \ell$, we can assume that p is unramified in M. Let $f_\pi = [M_\pi : \mathbb{Q}_p] = [k_\pi : \mathbb{F}_p]$ be the inertia degree of π. Now,

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

for an M_π-submodule $\hat{W}$ of $\hat{V}_\pi$. Also,

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

for a k_π-submodule W of V_π. Since

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

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

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

$$E : Y^2 + a_1XY + a_3Y = X^3 + a_2X^2 + a_4X + a_6,$$
$$E' : Y^2 + a_1'XY + a_3'Y = X^3 + a_2'X^2 + a_4'X + a_6',$$

where the a_i, a_i' lie in a discrete valuation ring $\mathcal{O}$ with uniformizer ν, 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 ν^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'. ■

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

$$E : Y^2 + a_1XY + a_3Y = X^3 + a_2X^2 + a_4X + a_6,$$
$$E' : Y^2 + a'_1XY + a'_3Y = X^3 + a'_2X^2 + a'_4X + a'_6,$$

where the a_i, a'_i lie in a discrete valuation ring $\mathcal{O}$ with uniformizer ν, and the valuation at ν 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 ν^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 and terminate at Step 1 (again because the valuation of the discriminant of the model for E' is equal to 12). ■

THEOREM 32. *The conductor of $E_\beta = E^s_\beta$ is*

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

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_β is given by

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

with

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

where

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

Let

$$\begin{aligned} c_4 &= -2^4 \cdot 3 \cdot -3\delta((3+2\sqrt{5})s - 3t)\gamma^2, \\ c_6 &= -2^5 \cdot 3^3 \cdot 4v((17-4\sqrt{5})s - (45-18\sqrt{5})t)\gamma^3. \end{aligned} \tag{15}$$

Let $\mathfrak{q}$ be a prime not dividing $2 \cdot 3 \cdot 5$ but dividing Δ_{E_β}. The elliptic curve E_β has multiplicative bad reduction at $\mathfrak{q}$ if one of $c_4, c_6 \not\equiv 0 \pmod{\mathfrak{q}}$. Since δ and γ 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

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

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_β 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 (14) we have $v_3(\Delta_{E_\beta}) = 6$. Hence, by [26, Tableaux II], (13) is in minimal form at $\mathfrak{q}_3$. We go through all possibilities for (v,t) modulo ν_3^4, and in each case we compute the reduction type of E_β at $\mathfrak{q}_3$ using MAGMA, which all turn out to be I_0^*. By Lemma 30, this determines all the possible conductor exponents for E_β at $\mathfrak{q}_3$.

We change the model for elliptic curve E_β by replacing γ by $\mu = \gamma/z^2$ in (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 purpose 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

$$\begin{aligned} Y^2 = X^3 &- 3\delta((3+2\sqrt{5})s - 3t)\mu^2 X \\ &+ 4v((17-4\sqrt{5})s - (45-18\sqrt{5})t)\mu^3 \end{aligned} \tag{16}$$

with

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

If $s \not\equiv 0 \pmod 5$, then by (17), we have $v_5(\Delta_{E_\beta}) = 6$ so (16) is minimal at $\mathfrak{q}_5$. We go through all possibilities for (v,t) modulo ν_5^4 subject to $s \not\equiv 0 \pmod 5$, and in each case we compute the reduction type of E_β at $\mathfrak{q}_5$ using MAGMA, which all turn out to be I_0^*. By Lemma 30, this determines all the possible conductor exponents for E_β at $\mathfrak{q}_5$. If $s \equiv 0 \pmod 5$, then $v_5(s) \geq 4$. It follows from (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_β which has good reduction at $\mathfrak{q}_5$.

Since $s \not\equiv t \pmod 2$, by (14) we see that $v_2(\Delta_{E_\beta}) = 12$. We go through all possibilities for (v, t) modulo ν_2^6, and in each case we compute the reduction type of E_β at $\mathfrak{q}_2$ using MAGMA, which all turn out to be II^* or I_0. By Lemma 31, this determines all the possible conductor exponents for E_β at $\mathfrak{q}_2$. ■

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

$$\mathfrak{m} = \mathfrak{q}_2^\alpha \cdot \mathfrak{q}_3^2 \cdot \mathfrak{q}_5^\varepsilon \cdot \prod_{\mathfrak{q} \mid s^2 - 10st + 5t^2}{}^{\!\!\prime} \; \mathfrak{q},$$

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_β is given by

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

with

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

where

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

Let

$$\begin{aligned} c_4 &= -2^4 \cdot 3 \cdot -3 \cdot 2^2 \cdot \sqrt{5}(3s - (15 - 10\sqrt{5})t)\gamma^2, \\ c_6 &= -2^5 \cdot 3^3 \cdot 2^5 \cdot 5u(9s - (45 - 14\sqrt{5})t)\gamma^3. \end{aligned}$$

Let $\mathfrak{q}$ be a prime not dividing $2 \cdot 3 \cdot 5$ but dividing Δ_{E_β}. The elliptic curve E_β has multiplicative bad reduction at $\mathfrak{q}$ if one of $c_4, c_6 \not\equiv 0 \pmod{\mathfrak{q}}$. Since γ 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

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

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_β 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 (19) we have $v_3(\Delta_{E_\beta}) = 6$. Hence, by [26, Tableaux II], (18) is in minimal form at $\mathfrak{q}_3$. We go through all possibilities for (u, s) modulo ν_3^4, and in each case we compute the reduction type of E_β at $\mathfrak{q}_3$ using MAGMA, which all turn out to be type I_0^*. By Lemma 30, this determines all the possible conductor exponents for E_β at $\mathfrak{q}_3$.

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

$$\begin{aligned}Y^2 = X^3 - 3 \cdot 2^2 \cdot \sqrt{5}(3s - (15 - 10\sqrt{5})t)\mu^2 X \\ + 2^5 \cdot 5u(9s - (45 - 14\sqrt{5})t)\mu^3\end{aligned} \tag{20}$$

with

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

If $s \not\equiv 0 \pmod 5$, then $v_5(\Delta_{E_\beta}) = 0$ so E_β has good reduction at $\mathfrak{q}_5$. If $s \equiv 0 \pmod 5$, then by (21), we have $v_5(\Delta_{E_\beta}) = 6$ so (20) is minimal at $\mathfrak{q}_5$. We go through all possibilities for (u, s) modulo ν_5^4 subject to $s \not\equiv 0 \pmod 5$, and in each case we compute the reduction type of E_β at $\mathfrak{q}_5$ using MAGMA, which all turn out to be type I_0^*. By Lemma 30, this determines all the possible conductor exponents for E_β at $\mathfrak{q}_5$.

We change the model for elliptic curve E_β by replacing γ by $\mu = \gamma/\nu_2^2$ in (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 purpose of computing the conductor exponent at $\mathfrak{q}_2$.

Since $s \not\equiv t \pmod 2$, then by (19) we see that $v_2(\Delta_{E_\beta}) = 12$. We go through all possibilities for (u, s) modulo ν_2^6, and in each case we compute the reduction type of E_β at $\mathfrak{q}_2$ using MAGMA, which all turn out to be II^* or I_0. By Lemma 31, this determines all the possible conductor exponents for E_β at $\mathfrak{q}_2$. ■

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

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

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. See [22, Lemma, p. 178]. We also note that K_β is unramified outside $\{2, 5\}$ so the product is of the form stated. ■

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

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

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. See [22, Lemma, p. 178]. We also note that K_β is unramified outside $\{2, 5\}$ so the product is of the form stated. ■

From now 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 $\{\hat{V}_\pi(\mathrm{Res}_{\mathbb{Q}}^{K_\beta} E_\beta)\}$ is one of

$$2^4 \cdot 3^4 \cdot 5^3 \prod_{q \mid s^2 - 10st + 5t^2}{}' q^2, \quad 2^8 \cdot 3^4 \cdot 5^3 \prod_{q \mid s^2 - 10st + 5t^2}{}' q^2,$$

using Theorems 34 and 35, and Lemmas 28 and 29.

We note that the trivial solution $s = 0, t = 1$ gives rise to the last case and $E_0 = E^s_\beta$ has complex multiplication by $\sqrt{-4}$ in this situation. The trivial solution $s = 1$, $t = 0$ gives rise to the first case and $E_1 = E^t_\beta$ 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 (cf. [7, Théorème 2.1], [8, Théorème (A)], [12, Theorem 3.1], [18, (0.1)]). *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* ψ*, 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* ψ*, then* $\hat{\rho}_{f,\pi}|_{D_q}$ *is of the form*

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

Here χ *is the unramified character of* D_ℓ *which sends* Fr_q *to* a_q *and* $\chi_p : G_\mathbb{Q} \to \mathbb{Z}_p^*$ *is the pth cyclotomic character.*

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 (see [2]). Let $f \in S_k(\Gamma_0(N), \psi)$ where ψ is a character of conductor $N' \mid N$. Let χ be a character of conductor M. Then the twist f_χ of f by χ lies in $S_k(\Gamma_0(\tilde{N}), \psi\chi^2)$ where $\tilde{N} = \mathrm{lcm}(N, N'M, M^2)$.

THEOREM 37 (cf. [2, Theorem 3.1]). *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 ψ_q of ψ is equal to q^α with $\alpha \geq 0$. Let χ be a character of conductor q^β with $\beta \geq 1$. Put $Q' = \max(Q, q^{\alpha+\beta}, q^{2\beta})$. Then*

- *f_χ is of level dividing $Q'M$,*
- *for each prime $q' \mid M$, f_χ is not of level $Q'M/q'$,*
- *the exact level of f_χ 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 $Q' > Q$.* ■

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

$$2^2 \cdot 3^2 \cdot 5 \prod_{q \mid s^2-10st+5t^2}{}' q = 180 \prod_{q \mid s^2-10st+5t^2}{}' q,$$
$$2^4 \cdot 3^2 \cdot 5 \prod_{q \mid s^2-10st+5t^2}{}' q = 720 \prod_{q \mid s^2-10st+5t^2}{}' q.$$

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_β so that $I_p \subseteq G_{K_\beta}$. ■

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 ℓ when $\ell \neq 2, 3, 5$, and in the case of multiplicative bad reduction, the exponent of a prime above ℓ in the minimal discriminant of E is divisible by p. Also, ℓ is unramified in K_β so that $I_\ell \subseteq G_{K_\beta}$. ■

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_β is unramified at ℓ and hence G_{K_β} contains I_ℓ. Now, in our case, $\rho|_{G_{K_\beta}}$ is isomorphic to $\phi_{E,p}$. Since $\phi_{E,p}|_{I_\ell}$ is trivial, we see that $\rho|_{I_\ell}$ is trivial so ρ 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 ℓ in the conductor of ρ is the same as in the conductor of $\hat{\rho}$ as $p \neq 2, 3$. ∎

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 ρ is determined by $\rho|_{I_p}$. Since $p \neq 2, 5$, we see that K_β is unramified at p and hence G_{K_β} 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 pth cyclotomic character, the weight of ρ is 2 [33, Proposition 4]. ∎

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

Proof. This follows from (1). ∎

THEOREM 43 (cf. [14, Proposition 3.2]). *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 $\ell > 3$.* ∎

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. ∎

THEOREM 45 (cf. [14, Proposition 3.4]). *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 $\ell > 3$.* ∎

We note in the context of [14, Propositions 3.2 and 3.4] that 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 $X^K_{0,B}(d,p)$, $X^K_{0,N}(d,p)$, $X^K_{0,N'}(d,p)$ be the modular curves with level p structure corresponding to a Borel subgroup B, to the normalizer of a split Cartan subgroup N, and to the normalizer of a non-split Cartan subgroup N' of $\mathrm{GL}_2(\mathbb{F}_p)$ respectively, and with 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*

- *the elliptic curve E is defined over K,*

- *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* $\sigma \notin G_K$*,*
- $\mu_E(\sigma)^{\sigma}\mu_E(\sigma) = \pm d$ *whenever* $\sigma \notin G_K$*.*

If $\rho_{E,\beta,\pi}$ *has image lying in a Borel subgroup, in the normalizer of a split Cartan subgroup, or in the 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 $\mathbb{P}\overline{\rho}_{E,p} : G_{\mathbb{Q}} \to \mathrm{PGL}_2(\mathbb{F}_p)$ is simply the projectivization of our $\rho_{E,\beta,\pi} : G_{\mathbb{Q}} \to \overline{\mathbb{F}}_p^{\times}\,\mathrm{GL}_2(\mathbb{F}_p)$ (this does not depend on the choice of β). 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 $\mu_E(\sigma)({}^{\sigma}C_p) = C_p$ 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 τ is an element of $G_{\mathbb{Q}}$ which is non-trivial on K. This does not depend on the choice of τ.

Suppose τ 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 $\mu_E(\tau)({}^{\tau}C_d) = \mu_E(\tau)^{\tau}\mu_E(\tau)({}^{\tau^2}E[d]) = [\pm d]({}^{\tau^2}E[d]) = 0$. 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 σ is an element of $G_{\mathbb{Q}}$ which is trivial on K. In this case, we have ${}^{\sigma}(E, C_d, C_p) = (E, C_d, C_p)$. 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 ${}^{\sigma}\mu_E(\tau) = \pm\mu_E(\sigma\tau) = \pm\mu_E(\tau)$ 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 that 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. ■

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 image of the representation* $\rho_{E,\beta,\pi}$ *does not lie 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. ■

It follows from work on the refined Serre 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 ${}^{\sigma}f = f \otimes \epsilon$ and ${}^{\sigma}f' = f' \otimes \epsilon$ where σ is the non-trivial automomorphism of $M = \mathbb{Q}(i)$ by [29, Example 3.7]. We have $G_{K_\beta/\mathbb{Q}} \cong (\mathbb{Z}/20\mathbb{Z})^*/\{\pm 1\} = \{\pm 1, \pm 3, \pm 7, \pm 9\}$ and ± 7 and ± 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 (cf. [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 $u + v = 0$, and if $q \equiv \pm 7 \pmod{20}$, then $u - v = 0$.

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

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

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 find 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 p.

A computation of $S_2(\Gamma_0(180), \epsilon^{-1})$ reveals two 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 three 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 four 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 three 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 using W. Stein's modular symbols package. They are posted at www.math.sfu.ca/˜ichen/x225-data for the reader's convenience.

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 $\rho_{f,\pi} \cong \rho_{g,\pi}$, 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 know 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 ϕ 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 GL_2-type defined over $\mathbb{Q}$ attached to C. We have shown that A_g is isogenous over $\mathbb{Q}$ to A_β for some splitting map β 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 β is as defined in (8), up to multiplication by a quadratic Galois character unramified outside $\{2,3,5\}$. Thus, K_β 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_β by the construction of A_β. 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 in a split Cartan subgroup of $\mathrm{GL}_2(k_\pi) = \mathrm{GL}_2(\mathbb{F}_p)$. This implies that in fact $\rho_{g,\pi}|_{G_F}$ has image 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, $\det\rho_{g,\pi}|_{G_L} = \overline{\epsilon}^{-1}\overline{\chi}_p$ is surjective to $\mathbb{F}_p^\times$ since L does not contain a primitive pth root of unity for $p > 5$. Finally, as $[G_{\mathbb{Q}} : G_F] = 2$ it follows that $\rho_{g,\pi}$ itself has image in the normalizer of a split Cartan subgroup of $\mathrm{GL}_2(\mathbb{F}_p)$ by the classification of subgroups of $\mathrm{GL}_2(\mathbb{F}_p)$. ■

6. The inapplicability of Mazur's method in the non-split Cartan case. Let d be a prime and $d \neq p$. Let χ 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 $X^K_{0,N'}(d,p)$ 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 $J^K_{0,N'}(d,p)$ be the jacobian of $X^K_{0,N'}(d,p)$.

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

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

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

$$\pi_1 : J_{0,N'}(d,p) \to \prod_{[f]\in N_2^+(\Gamma_0(p^2))} A_{[f]},$$

$$\pi_2 : J_{0,N'}(d,p) \to \prod_{[f]\in N_2^+(\Gamma_0(p^2))} A_{[f]},$$

$$\pi_3 : J_{0,N'}(d,p) \to \prod_{[f]\in N_2^{+,+}(\Gamma_0(dp^2))} A_{[f]},$$

$$\pi_4 : J_{0,N'}(d,p) \to \prod_{[f]\in N_2^{-,+}(\Gamma_0(dp^2))} A_{[f]}$$

be the homomorphisms obtained by composing the projection to the given group of factors with π. Then $\pi_i \circ w_d = \pi_i$ 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 χ is obtained through the action of w_d on $X_{0,N'}(d,p)$. Hence, $J^K_{0,N'}(d,p)$ 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 χ a character of conductor m prime to N. Then f_χ is a newform in $S_k(\Gamma_0(Nm^2), \epsilon\chi^2)$ and*

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

Proof. See the statement in [2, p. 228] based on a theorem of Weil [39] stated in [21, Theorem 6]. ∎

Suppose K is real, d is inert in K, and the conductor of χ 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 $N = dp^2$. Then $\chi(-p^2) = 1$ and $\chi(-dp^2) = -1$. For $[f] \in N_2^+(\Gamma_0(p^2))$, $\lambda_{p^2m^2}(f_\chi) = \chi(-p^2)\lambda_{p^2}(f) = 1$ by Theorem 49. For $[f] \in N_2^{-,+}(\Gamma_0(dp^2))$, $\lambda_{dp^2m^2}(f_\chi) = \chi(-dp^2)\lambda_{dp^2}(f) = 1$ 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:

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

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

$$j = (t+256)^3/t^2, \qquad j - 1728 = \frac{(t+64)(t-512)^2}{t^2},$$

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 ℓ-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 ℓ-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.

Acknowledgements. I would like to thank M. Bennett, J. Ellenberg, S. Siksek, C. Skinner for many useful discussions and suggestions. I would also like to 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 my visits there in 2006–2007.

This research was supported by NSERC.

References

[1] *Groupes de monodromie en géométrie algébrique. I*, 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 Math. 288, Springer, Berlin, 1972.

[2] A. O. L. Atkin and W.-C. Li, *Twists of newforms and pseudo-eigenvalues of W-operators*, Invent. Math. 48 (1978), 221–243.

[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*, Canad. J. Math. 56 (2004), 23–54.

[5] W. Bosma, J. Cannon, and C. Playoust, *The Magma algebra system. I. The user language*, in: Computational Algebra and Number Theory (London, 1993), J. Symbolic Comput. 24 (1997), 235–265.

[6] J. Buhler and B. Gross, *Arithmetic on elliptic curves with complex multiplication II*, Invent. Math. 79 (1985), 11–29.

[7] H. Carayol, *Sur les représentations l-adiques attachés aux formes modulaires de Hilbert*, C. R. Acad. Sci. Paris Sér. I 296 (1983), 629–632.

[8] —, *Sur les représentations p-adiques associées aux formes modulaires de Hilbert*, Ann. Sci. École Norm. Sup. 19 (1986), 409–468.

[9] I. Chen, *On the equation $s^2 + y^{2p} = \alpha^3$*, Math. Comp. 77 (2007), 1223–1227.

[10] C. Cummins and S. Pauli, *Congruence subgroups of $PSL(2, \mathbb{Z})$ of genus less than or equal to* 24, Experiment. Math. 12 (2003), 243–255.

[11] H. Darmon, *Rigid local systems, Hilbert modular forms, and Fermat's Last Theorem*, Duke Math. J. 102 (2000), 413–449.

[12] H. Darmon, F. Diamond, and R. Taylor, *Fermat's Last Theorem*, in: Elliptic Curves, Modular Forms & Fermat's Last Theorem (Hong Kong, 1993), Int. Press, 1997, 2–140.

[13] H. Darmon and L. Merel, *Winding quotients and some variants of Fermat's Last Theorem*, J. Reine Angew. Math. 490 (1997), 81–100.

[14] J. Ellenberg, *Galois representations attached to $\mathbb{Q}$-curves and the generalized Fermat equation $A^4 + B^2 = C^p$*, Amer. J. Math. 126 (2004), 763–787.

[15] J. Ellenberg and C. Skinner, *On the modularity of $\mathbb{Q}$-curves*, Duke Math. J. 109 (2001), 97–122.

[16] A. Granville and H. Darmon, *On the equations $x^p + y^q = z^r$ and $z^m = f(x, y)$*, Bull. London Math. Soc. 27 (1995), 513–544.

[17] B. Gross, *Arithmetic on Elliptic Curves with Complex Multiplication*, Lecture Notes in Math. 776, Springer, 1980.

[18] —, *A tameness criterion for Galois representations associated to modular forms (mod p)*, Duke Math. J. 61 (1990), 445–517.

[19] A. Kraus, *Sur l'équation $a^3 + b^3 = c^p$*, Experiment. Math. 7 (1998), 1–13.

[20] —, *On the equation $x^p + y^q = z^r$: A survey*, Ramanujan J. 3 (1999), 315–333.

[21] W. Li, *Newforms and functional equations*, Math. Ann. 212 (1975), 285–315.

[22] J. Milne, *On the arithmetic of abelian varieties*, Invent. Math. 17 (1972), 177–190.

[23] T. Miyake, *Modular Forms*, Springer, 1989.

[24] H. Montgomery and P. Weinberger, *Notes on small class numbers*, Acta Arith. 24 (1973/74), 529–542.

[25] A. P. Ogg, *Elliptic curves and wild ramification*, Amer. J. Math. 89 (1967), 1–21.

[26] I. Papadopoulos, *Sur la classification de Néron des courbes elliptiques en caractéristique résiduelle* 2 *et* 3, J. Number Theory 44 (1993), 119–152.

[27] J. Quer, *$\mathbb{Q}$-curves and abelian varieties of GL_2-type*, Proc. London Math. Soc. 81 (2000), 285–317.

[28] K. Ribet, *Galois representations attached to eigenforms with nebentypus*, in: Modular Functions of One Variable V (Bonn, 1976), Lecture Notes in Math. 601, Springer, 1972, 17–51.

[29] —, *Twists of modular forms and endomorphisms of abelian varieties*, Math. Ann. 253 (1980), 43–62.

[30] —, *Abelian varieties over $\mathbb{Q}$ and modular forms*, in: Algebra and Topology 1992, Korea Adv. Inst. Sci. Tech., 1992, 53–79.

[31] J.-P. Serre, *Corps locaux*, 2nd ed., Publications Univ. Nancago 8, Hermann, Paris, 1968.

[32] —, *Modular forms of weight one and Galois representations*, in: A. Fröhlich (ed.), Algebraic Number Fields, Academic Press, 1977, 193–268.

[33] —, *Sur les représentations modulaires de degré* 2 *de* $\mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})$, Duke Math. J. 54 (1987), 179–230.

[34] J.-P. Serre and J. Tate, *Good reduction of abelian varieties*, Ann. of Math. 88 (1968), 492–517.

[35] G. Shimura, *On elliptic curves with complex multiplication as factors of the jacobians of modular function fields*, Nagoya Math. J. 43 (1971), 199–208.

[36] J. H. Silverman, *Advanced Topics in the Arithmetic of Elliptic Curves*, Springer, 1994.

[37] H. Stark, *On complex quadratic fields with class-number two*, Math. Comp. 29 (1975), 289–302.

[38] M.-F. Vignéras, *Arithmétique des algèbres de quaternions*, Lecture Notes in Math. 800, Springer, 1980.

[39] A. Weil, *Über die Bestimmung Dirichletscher Reihen durch Funktionalgleichungen*, Math. Ann. 168 (1967), 149–156.

Imin Chen
Department of Mathematics
Simon Fraser University
Burnaby, British Columbia, Canada V5A 1S6
E-mail: ichen@math.sfu.ca

Received on 22.4.2008
and in revised form on 19.4.2010 (5691)