Introduction to \( \mathbb{Q} \)-curves

Imin Chen
Simon Fraser University
ichen@math.sfu.ca

November 24, 2008
Introduction

Some Galois cohomology

Abelian varieties of $GL_2$-type

Explicit splitting maps for example

References
• 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 by [Gross-1980] [Buhler-Gross-1985] but was extended by Ribet [Ribet-1992] to the non-CM case using different methods.

• Further explicit considerations were developed in [Quer-2000] which we will use in the sequel.

• The exposition below of the theory follows closely the citations above as well as [Ellenberg-Skinner-2001].
• \( \mathbb{Q} \)-curves are interesting classes of elliptic curves over number fields because their ‘isogeny class’ is defined over \( \mathbb{Q} \).

• A priori, if one has an elliptic curve \( C \) defined over a number field \( K \), one can attach Galois representations \( \phi_{C,p} : G_K \rightarrow \text{GL}_2(\mathbb{Q}_p) \) of \( G_K \) from its Tate modules.

• If \( C \) is a \( \mathbb{Q} \)-curve, we will explain how one can attach a Galois representation \( \rho_{C,\beta,\pi} : G_\mathbb{Q} \rightarrow \overline{\mathbb{Q}}_p^* \text{GL}_2(\mathbb{Q}_p) \).

• This allows us to make sense of the modularity of \( C \) using classical modular forms \( f \in S_2(\Gamma_0(N), \epsilon) \), rather than going into the realm of more general automorphic forms.

• \( \mathbb{Q} \)-curves are thus one form of generalization of the notion of a modular elliptic curve over \( \mathbb{Q} \).
Consider the elliptic curve $C$ defined over $\mathbb{Q}(\sqrt{5})$ given by where $u, v \in \mathbb{Q}$.

$$C : Y^2 = X^3 - 3 \left( \frac{-5 + 3\sqrt{5}}{2} \right) \left( (3 + 2\sqrt{5})v^2 - 3u^2 \right) X$$

$$+ 4v \left( (17 - 4\sqrt{5})v^2 - (45 - 18\sqrt{5})u^2 \right).$$

Its discriminant is

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

where $s = v^2$, $t = u^2$, $\eta = \kappa^{-3}$, $\kappa = -\frac{1+\sqrt{5}}{2}$, which we require to be non-zero.

The elliptic curve $C$ has a 2-torsion point defined over $\mathbb{Q}(\sqrt{5})$ given by

$$(X, Y) = ((2\sqrt{5} - 2)v, 0).$$
Replacing $X$ by $X + (2\sqrt{5} - 2)v$ gives a model where the 2-torsion point defined over $\mathbb{Q}(\sqrt{5})$ is now $(X, Y) = (0, 0)$. The equation of $C$ is now

$$Y^2 = X^3 + \left((6\sqrt{5} - 6)v\right) X^2$$

$$+ \left(\frac{27\sqrt{5} - 45}{2} u^2 + \frac{-45\sqrt{5} + 99}{2} v^2\right) X.$$

Recall if $E$ is an elliptic curve given by $Y^2 = X^3 + aX^2 + bX$ and $\phi : E \to E'$ is the 2-isogeny with kernel equal to the subgroup $\langle (0, 0) \rangle$, then $E'$ is given by $Y^2 = X^3 + AX^2 + BX$ where $A = -2a$, $B = a^2 - 4b$, and $\phi(X, Y) = (Y^2/X^2, Y(b - X^2)/X^2)$. 


Let $\sigma$ be an automorphism such that $\sigma(\sqrt{5}) = -\sqrt{5}$. Consider the conjugate $\sigma C$ given by

$$Y^2 = X^3 + \left(( - 6\sqrt{5} - 6)\nu \right) X^2$$

$$+ \left(\frac{-27\sqrt{5} - 45}{2} u^2 + \frac{45\sqrt{5} + 99}{2} \nu^2 \right) X.$$

Taking the quotient by the subgroup $\langle (0,0) \rangle$, we see that $\sigma C$ is 2-isogenous over $\mathbb{Q}(\sqrt{5})$ to the elliptic curve $C'$ given by

$$Y^2 = X^3 + \left((12\sqrt{5} + 12)\nu \right) X^2$$

$$+ \left((54\sqrt{5} + 90)u^2 + (-18\sqrt{5} + 18)\nu^2 \right) X.$$
• Let \( \alpha = \frac{1+\sqrt{5}}{\sqrt{2}} \). Then \( \psi(X, Y) = (X\alpha^2, Y\alpha^3) \) gives an isomorphism \( \psi : C' \to C \) defined over \( \mathbb{Q}(\sqrt{5}, \sqrt{2}) \).

• Thus, there is a 2-isogeny \( \sigma : C \to C \) defined over \( \mathbb{Q}(\sqrt{5}, \sqrt{2}) \).

• \( C \) is thus a \( \mathbb{Q} \)-curve defined over \( \mathbb{Q}(\sqrt{5}, \sqrt{2}) \), but not over \( \mathbb{Q}(\sqrt{5}) \), even though \( C \) is defined over \( \mathbb{Q}(\sqrt{5}) \).

• 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 \( G_K \).

• In our example, we take \( K = \mathbb{Q}(\sqrt{5}, \sqrt{2}) \). If \( \sigma(\sqrt{5}) = \sqrt{5} \), then \( \sigma C = C \) and we take \( \mu(\sigma) = 1 \). If \( \sigma(\sqrt{5}) = -\sqrt{5} \), then we take \( \mu(\sigma) \) to be the 2-isogeny \( \sigma : C \to C \) described earlier.
• \( \mathbb{Q} \)-curves have applications to resolving diophantine equations, for instance, special classes of the generalized Fermat equation

\[
Ax^a + By^b = Cz^c.
\]

• This was first used in [Ellenberg-2004] to resolve the case

\[
x^2 + y^4 = z^p.
\]

• The idea is to apply a version of the “modular method” which uses \( \mathbb{Q} \)-curves.

• For example, suppose we wish to resolve an equation such as

\[
x^2 + y^{2p} = z^5.
\]
• One first tries to construct ‘Frey curves’ for this class of equations, which means we try to attach to each non-trivial proper solution a curve which gives rise to a Galois representation which has bounded ramification independent of the solution and exponents in the class.

• Assuming we can show their modularity, the problem is then reduced to one of rational points on modular curves and/or congruences between modular forms.

• It turns out for the equation $x^2 + y^{2p} = z^5$, one choice of ‘Frey curve’ is the $\mathbb{Q}$-curve example given previously [Chen-2007].

• Because it is a $\mathbb{Q}$-curve, we can attach a Galois representation $\rho_{C,\beta,\pi} : \text{Gal}(\overline{\mathbb{Q}}/\mathbb{Q}) \to \text{GL}_2(\overline{\mathbb{Q}}_p)$ to it, prove its modularity, and then apply the modular method.
Using classical descent, one can show non-trivial proper solutions to \( x^2 + y^{2p} = z^5 \) for an odd prime \( p \) give rise to solutions to

- \( s^2 - 10st + 5t^2 = 5^j \gamma^p \) 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 \( k \geq 1 \)
- \( s = v^2, t = u^2 \)
- \( (s, t) = 1 \).

If we look at the discriminant of \( C \), it has the form

\[
\Delta_C = 2^6 \cdot 3^6 \cdot \eta^{-3} \cdot \left( s - (5 + 2\sqrt{5})t \right)^2 \left( s - (5 - 2\sqrt{5})t \right).
\]

This shows \( C \) has the properties to be a ‘Frey curve’ for the equation \( x^2 + y^{2p} = z^5 \).
• The example we considered was such that $C$ was defined over a quadratic extension $K$ and the non-trivial conjugate $\sigma C$ was 2-isogenous to $C$ over $\overline{\mathbb{Q}}$.

• Such examples are classified by the $\mathbb{Q}$-rational points on the modular curve $X_0(2)/\langle w_2 \rangle$, where $w_2$ is the Fricke involution on $X_0(2)$.

• If we want to specify the quadratic extension, such examples are classified by the $\mathbb{Q}$-rational points on the twist $X_0(2)^\chi$ of $X_0(2)$ by the cocycle in $H^1(G_{\mathbb{Q}}, \text{Aut}(X_0(2)))$ given by

$$\chi : G_{\mathbb{Q}} \to \{\pm 1\} \cong \langle w_2 \rangle \subseteq \text{Aut}(X_0(2)),$$

where $\chi$ is the character associated to the quadratic extension $K$. 
• Both $X_0(2)$ and $X_0(2)/\langle w_2 \rangle$ have genus 0 and are isomorphic to $\mathbb{P}^1$.
• If $t$ is a uniformizer for $X_0(2)$, then the map $X_0(2) \to X(1)$ is given by $j = \frac{(t+256)^3}{t^2}$.
• If $s$ is a uniformizer for $X_0(2)/\langle w_2 \rangle$, then the correspondence between $X_0(2)/\langle w_2 \rangle$ and $X(1)$ is given by
\[
j^2 + (-s^2 - 49s + 6656)j + s^3 + 816t^2 + 221952s + 20123648 = 0,
\]
and $s = t + 4096/t$. 
• When we speak of a $\mathbb{Q}$-curve, we will assume that it does not have complex multiplication.

• In our example, $C$ will have complex multiplication if and only if
  1. $v/u = 0, j_C = 1728, d(O) = -4$
  2. $v/u = \pm 1, j_C = 8000, d(O) = -8$
  3. $v/u = \pm 3, j_C = 212846400 + 95178240\sqrt{5}, d(O) = -40$
  4. $v/u = \infty, j_C = 632000 + 282880\sqrt{5}, d(O) = -20
This follows from the formula from the $j$-invariant of $C$.

$$j_C = \frac{2^6 \cdot 5\sqrt{5} \cdot \eta \cdot ((3 + 2\sqrt{5})s - 3t)^3}{(s - (5 + 2\sqrt{5})t)^2 (s - (5 - 2\sqrt{5})t)}$$

(1)

where $s = v^2$, $t = u^2$, $\eta = \kappa^{-3}$, $\kappa = \frac{-1+\sqrt{5}}{2}$.

Assume $s/t \in \mathbb{Q}$. Then $j_C$ does not lie in $\mathbb{Q}$ unless

- $s/t = 0, j_C = 1728$
- $s/t = 1, j_C = 8000.$
The elliptic curves with complex multiplication by an imaginary quadratic order $\mathcal{O}$ of class number 2 are listed below (c.f. [Montgomery-Weinberger-1973], [Stark-1975]).

$$
\begin{array}{|c|c|}
\hline
d(\mathcal{O}) & j \\
\hline
-15 & (-191025 \pm 85995\sqrt{5})/2 \\
-20 & 63200 \pm 28288\sqrt{5} \\
-24 & 2417472 \pm 1707264\sqrt{2} \\
-35 & -58982400 \pm 26378240\sqrt{5} \\
-40 & 212846400 \pm 95178240\sqrt{5} \\
-51 & -2770550784 \pm 671956992\sqrt{17} \\
-52 & 3448440000 \pm 956448000\sqrt{13} \\
-88 & 3147421320000 \pm 2225561184000\sqrt{2} \\
-91 & -5179536506880 \pm 143654958464\sqrt{13} \\
-115 & -213932305612800 \pm 9567343586560\sqrt{5} \\
-123 & -677073420288000 \pm 105741103104000\sqrt{41} \\
-148 & 19830091900536000 \pm 326004705936000\sqrt{37} \\
-187 & -2272668190894080000 \pm 55120300017868800\sqrt{17} \\
-232 & 302364978924945672000 \pm 5614776700979846400\sqrt{29} \\
-235 & -411588709724712960000 \pm 184068066743177379840\sqrt{5} \\
-267 & -9841545927039744000000 \pm 1043201781864732672000\sqrt{89} \\
-403 & -1226405694614665695989760000 \pm 340143739727246741938176000\sqrt{13} \\
-427 & -7805727756261891959906304000 \pm 999421027517377348595712000\sqrt{61} \\
\hline
\end{array}
$$
For a left $G$-module $M$, recall $H^0(G, M) = Z^0(G, M)/B^0(G, M)$ where

- $Z^0(G, M) = \{ \phi : G \to M \mid \phi^{-1} \sigma \phi = 1 \}$,
- $B^0(G, M) = \{1\}$.

So we see that $H^0(G, M) = ^G M$. In fact, it is probably better to take the point of view that $H^0(G, M) := ^G M$ (see later slide about short exact sequences giving rise to long exact sequences).
For a left $G$-module $M$, recall $H^1(G, M) = Z^1(G, M)/B^1(G, M)$ where

- $Z^1(G, M) = \{ \phi : G \to M \mid \phi(\sigma)^\sigma \phi(\tau) \phi(\sigma \tau)^{-1} = 1 \}$ the submodule of 1-cocycles,
- $B^1(G, M) = \{ \psi^{-1} \sigma \psi \mid \psi \in M \}$ the submodule of 1-coboundaries.

If we let $b(\sigma) = \psi^{-1} \sigma \psi$, then we see that

$$b(\sigma)^\sigma b(\tau) b(\sigma \tau)^{-1} = \psi^{-1} \sigma \psi^\sigma (\psi^{-1} \tau \psi) (\psi^{-1} \sigma \tau \psi)^{-1}$$
$$= \psi^{-1} \sigma \psi^\sigma \psi^{-1} \sigma \tau \psi^\sigma \tau \psi^{-1} \psi$$
$$= 0.$$

The other thing to note is that we can generalize the construction to allow for more general objects than $\psi \in M$ in the formula $b(\sigma) = \psi^{-1} \sigma \psi$. More precisely, let $\psi \in X$ where $X$ has a left action of $G$ and is a right $M$-torsor. Then $b(\sigma) = \psi^{-1} \sigma \psi$ will formally satisfy the conditions to be in $Z^1(G, M)$ and the different choices for $\psi$ will modify $b(\sigma)$ by a 1-coboundary. Thus, there is a well-defined class $b(\sigma) = \psi^{-1} \sigma \psi \in H^1(G, M)$ attached to $\psi \in X$. 


For a left $G$-module $M$, recall $H^2(G, M) = Z^2(G, M)/B^2(G, M)$ where

- $Z^2(G, M) = \{\phi : G \times G \to M \mid \phi(\sigma, \tau)\phi(\sigma\tau, \rho) = \sigma\phi(\tau, \rho)\phi(\sigma, \tau\rho)\}$ is the submodule of 2-cocycles,

- $B^2(G, M) = \{\psi(\sigma)\sigma\psi(\tau)\psi(\sigma\tau)^{-1} \mid \psi : G \to M\}$ is the submodule of 2-coboundaries.

If we let $c(\sigma, \tau) = \psi(\sigma)\sigma\psi(\tau)\psi(\sigma\tau)^{-1}$, then we see that

\[
c(\sigma, \tau)c(\sigma\tau, \rho)c(\sigma, \tau\rho)^{-1}\sigma c(\tau, \rho)^{-1}
\]
\[
= \psi(\sigma)\sigma\psi(\tau)\psi(\sigma\tau)^{-1}\psi(\sigma\tau)^{\sigma\tau}\psi(\rho)\psi(\sigma\tau\rho)^{-1}
\]
\[
\psi(\sigma\tau\rho)^{\sigma}\psi(\tau\rho)^{-1}\psi(\sigma)^{-1}\sigma\psi(\tau\rho)^{\sigma\tau}\psi(\rho)^{-1}\sigma\psi(\tau)^{-1}
\]
\[
= \psi(\sigma)\sigma\psi(\tau)^{\sigma\tau}\psi(\rho)^{\sigma}\psi(\tau\rho)^{-1}\psi(\sigma)^{-1}\sigma\psi(\tau\rho)^{\sigma\tau}\psi(\rho)^{-1}\sigma\psi(\tau)^{-1}
\]
\[
= \psi(\sigma)\sigma\psi(\tau)^{\sigma\tau}\psi(\rho)^{\sigma}\psi(\tau\rho)^{-1}\sigma\psi(\tau\rho)^{\sigma\tau}\psi(\rho)^{-1}\sigma\psi(\tau)^{-1}\psi(\sigma)^{-1}
\]
\[
= 1
\]
The last line uses the fact that

$$\psi(\sigma)^{-1} \sigma c(\tau, \rho)^{-1} = \sigma c(\tau, \rho)^{-1} \psi(\sigma)^{-1}$$

as $M$ is abelian. As before, we can allow for more general objects than $\psi : G \to M$ in the formula $c(\sigma, \tau) = \psi(\sigma)^{\sigma} \psi(\tau) \psi(\sigma \tau)^{-1}$ to produce classes in $H^2(G, M)$, as we will in our application.
Let
\[ 1 \rightarrow A \rightarrow B \rightarrow C \rightarrow 1 \]
be a short exact sequence of $G$-modules. This gives rise to an exact sequence
\[ 1 \rightarrow G^A \rightarrow G^B \rightarrow G^C, \]
we can view as
\[ 1 \rightarrow H^0(G, A) \rightarrow H^0(G, B) \rightarrow H^0(G, C). \tag{2} \]
The defining property of the cohomology groups $H^q(G, M)$ is that this extends to a long exact sequence
\[ 1 \rightarrow H^0(G, A) \rightarrow H^0(G, B) \rightarrow H^0(G, C) \]
\[ \quad \rightarrow H^1(G, A) \rightarrow H^1(G, B) \rightarrow H^1(G, C) \]
\[ \quad \rightarrow H^2(G, A) \rightarrow H^2(G, B) \rightarrow H^2(G, C) \rightarrow \ldots. \]
In fact, it can be shown there exists one and only one (up to canonical equivalence) cohomological extension of (2) (see Atiyah-Wall in Brighton Notes).
The maps $H^q(G, A) \to H^q(G, B)$ and $H^q(G, B) \to H^q(G, C)$ are the evident ones induced from the maps $A \to B$ and $B \to C$. The map $\delta : H^q(G, C) \to H^{q+1}(G, A)$ is called a connecting homomorphism.

- The connecting homomorphism $\delta : H^0(G, C) \to H^1(G, A)$ is given by $\delta(\phi)(\sigma) = \phi^{-1} \sigma \phi$ where $\phi \in Z^0(G, C)$.
- We know $\phi^{-1} \sigma \phi = 1$ as elements of $C$ so $\phi^{-1} \sigma \phi \in A$.
- The connecting homomorphism $\delta : H^1(G, C) \to H^2(G, A)$ is given by $\delta(\phi)(\sigma, \tau) = \phi(\sigma) \sigma \phi(\tau) \phi(\sigma \tau)^{-1}$ where $\phi \in Z^1(G, C)$.
- We know $\phi(\sigma)^\sigma \phi(\tau) \phi(\sigma \tau)^{-1} = 1$ as elements of $C$ so $\phi(\sigma)^\sigma \phi(\tau) \phi(\sigma \tau)^{-1} \in A$. 


• In the case of $G = G_K = \text{Gal}(\overline{K}/K)$, where $K$ is a number field,

$$G \cong \lim \leftarrow \text{Gal}(L/K)$$

is profinite where the inverse system run through all finite Galois extensions $L/K$. The topology on $G$ is given by a basis of open subsets containing the identity which consists of normal subgroups of finite index.

• We then require that the functions $\phi$ and $\psi$ are continuous where we put the discrete topology on $M$. 
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 \( \mu_C^{-1} := (1/ \text{deg} \mu_C) \mu'_C \) and \( \mu'_C \) is the dual of \( \mu_C \).

Then \( c_C(\sigma, \tau) \) determines a class in \( H^2(G\mathbb{Q}, \mathbb{Q}^*) \). More precisely, \( c_C(\sigma, \tau) \in Z^2(G\mathbb{Q}, \mathbb{Q}^*) \) and making different choices for \( \mu_C(\sigma) \) modifies this 2-cocycle by a 2-coboundary in \( B^2(G\mathbb{Q}, \mathbb{Q}^*) \).

This is because for any two \( \mu_C(\sigma), \mu'_C(\sigma) \in \text{Hom}(\sigma C, C) \otimes \mathbb{Q} \) we have that \( \mu'_C(\sigma) = \mu_C(\sigma) b(\sigma) = b(\sigma) \mu_C(\sigma) \) for \( b(\sigma) \in \mathbb{Q}^* \).
• The class of $c_C(\sigma, \tau) \in H^2(G_{\overline{\mathbb{Q}}}, \mathbb{Q}^*)$ only depends on the $\overline{\mathbb{Q}}$-isogeny class of $C$.

• This follows from the isomorphism between

$$\text{Hom}(\sigma C, C) \otimes \mathbb{Q} \rightarrow \text{Hom}(\sigma C', C') \otimes \mathbb{Q}$$

given by $f \mapsto \lambda^{-1} f^\sigma \lambda$ where $\lambda : C' \rightarrow C$ is an isogeny.
• If $C$ is a $\mathbb{Q}$-curve defined over $K$, then the class $c_C(\sigma, \tau)$ factors through $H^2(G_K/\mathbb{Q}, \mathbb{Q}^*)$ and only depends on the $K$-isogeny class of $C$.

• The class $c_C(\sigma, \tau)$ in fact lies in $H^2(G_\mathbb{Q}, \mathbb{Q}^*)[2]$.

• This follows by taking degrees of the formula

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

we get the identity

$$d(\sigma)d(\tau)d(\sigma \tau)^{-1} = c_C(\sigma, \tau)^2,$$

where $d(\sigma)$ is the degree of $\mu_C(\sigma)$. 
• Tate (cf. [Serre-1977-weight-one, Theorem 4]) showed that $H^2(G_{\mathbb{Q}}, \mathbb{Q}^*)$ is trivial where the action of $G_{\mathbb{Q}}$ on $\mathbb{Q}^*$ is trivial.

• Thus, there is a continuous map $\beta : G_{\mathbb{Q}} \rightarrow \mathbb{Q}^*$ such that

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

as elements of $Z^2(G_{\mathbb{Q}}, \mathbb{Q}^*)$, not just as classes in $H^2(G_{\mathbb{Q}}, \mathbb{Q}^*)$.

• In such a case, we say that $\beta$ is a splitting map for $C$ (or more precisely, for the cocycle $c_C(\sigma, \tau)$).
• 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 on the function $\mu_C$. 

The only thing to check is that the multiplication given on $R_C$ is associative. This follows from the computation below.

\[
(\lambda_\sigma \lambda_\tau) \lambda_\rho = \lambda_\sigma \lambda_\tau c_C(\sigma, \tau)^{-1} \lambda_\rho \\
= c_C(\sigma, \tau)^{-1} c_C(\sigma \tau, \rho)^{-1} \lambda_{\sigma \tau \rho}
\]

\[
\lambda_\sigma (\lambda_\tau \lambda_\rho) = \lambda_\sigma c_C(\tau, \rho)^{-1} \lambda_\tau \lambda_\rho \\
c_C(\tau, \rho)^{-1} c_C(\sigma, \tau \rho)^{-1} \lambda_{\sigma \tau \rho}
\]

Because we have

\[
c_C(\sigma, \tau) c_C(\sigma \tau, \rho) = \sigma c_C(\tau, \rho) c_C(\sigma, \tau \rho) = c_C(\tau, \rho) c_C(\sigma, \tau \rho),
\]

both sides are equal.
Consider the restriction of scalars $\text{Res}^K_Q C$, for which we recall its defining functorial property that

$$\text{Hom}(S, \text{Res}^K_Q C) \leftrightarrow \text{Hom}(S \otimes K, C).$$

There is a natural isomorphism

$$\mathcal{R}_C \rightarrow \text{End}_Q \text{Res}^K_Q C$$

which sends $\lambda_{\sigma}$ to the endomorphism of $\text{Res}^K_Q C$ defined by

$$P \mapsto \tau_{\mu_C}(\sigma)(P)$$
on $\sigma^\tau C$.

A simple example is $C = \text{Spec}(\mathbb{Q}(\sqrt{5})[X])$. Write

$$X = X_1 + X_2\sqrt{5}. \text{ Then } \text{Res}^\mathbb{Q}(\sqrt{5})_Q C = \text{Spec}(\mathbb{Q}[X_1, X_2]).$$

Another simple example is $C = \text{Spec}(\mathbb{Q}[X]/(X^2 - 5))$. Write

$$X = X_1 + X_2\sqrt{5}. \text{ Then } \text{Res}^\mathbb{Q}(\sqrt{5})_Q C = \text{Spec}(\mathbb{Q}[X_1, X_2]/(X_1^2 + 5X_2^2 - 5, 2X_1X_2)).$$
• Given a splitting map $\beta$ for $C$, we now enlarge $K$ if necessary so that $\beta$ factors through $G_{K/Q}$.
• The map given by $\theta_\beta : \lambda_\sigma \mapsto \beta(\sigma)$ gives a surjective homomorphism $\theta_\beta : R_C \to M_\beta = \mathbb{Q}(\beta(\sigma))$.
• This is because $c_C(\sigma, \tau) = \beta(\sigma)\beta(\tau)\beta(\sigma \tau)^{-1}$ so from the identity
  $$\lambda_\sigma \lambda_\tau = c_C(\sigma, \tau)\lambda_{\sigma \tau},$$
we obtain after applying $\theta_\beta$, the identity
  $$\beta(\sigma)\beta(\tau) = c_C(\sigma, \tau)\beta(\sigma \tau)$$
holds, which shows
  $$\theta_\beta(\lambda_\sigma)\theta_\beta(\lambda_\tau) = \theta_\beta(\lambda_{\sigma \tau}).$$
• As $R_C$ is a semi-simple $\mathbb{Q}$-algebra, there is a projection from $R_C$ onto the isomorphic copy of $M_\beta$ in $R_C$.
• 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 we need to find a $\beta(\sigma)$ so that

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

as cocycles in $Z^2(G_{\mathbb{Q}}, \mathbb{Q}^*)$ and $K$ needs to be large enough so $\beta(\sigma)$ factors through $G_{K/\mathbb{Q}}$.

• Suppose that as 2-cocycles we have have found a $\beta(\sigma)$ such 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 $\sqrt{\gamma}/\sqrt{\gamma}$ where $\gamma \in \overline{\mathbb{Q}}^*$.
• By the way twisting affects the cocycles $c_C(\sigma, \tau)$ [Quer-2000, p. 291] we see that the twist $C_\gamma$ of $C$ is such that

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

• By the twist $C_\gamma$ we mean if $C$ is given by $Y^2 = X^3 + AX + B$, then $C_\gamma$ is given by $Y^2 = X^3 + A\gamma^2X + B\gamma^3$.

• Thus, replacing $C$ by $C_\gamma$ allows us to use the $\beta(\sigma)$ given and we take $K$ be large enough so that $\beta(\sigma)$ factors through $G_K/\mathbb{Q}$.

• This will be useful because the splitting map $\beta(\sigma)$ for $c_{C_\gamma}(\sigma, \tau)$ might factor through a smaller field $K/\mathbb{Q}$ than a splitting map for $c_C(\sigma, \tau)$. 
• Recall an abelian variety defined over \( \mathbb{Q} \) of 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 GL\(_2\)-type attached to a \( \mathbb{Q} \)-curve \( C \) is one which has \( C \) as a quotient over \( \overline{\mathbb{Q}} \).

**Theorem**

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

**Proof.**

cf. [Ribet-1992, Theorem 6.1].
Proposition

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 $A_{\beta}$ 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 $A \to \text{Res}_K^Q C$ 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 $\text{Res}_K^Q C$. As $\mathcal{R}_C$ is a semi-simple $\mathbb{Q}$-algebra, there is a projection $\mathcal{R}_C \to \text{End}_\mathbb{Q} A$ given by $\lambda_\sigma \to \beta(\sigma)$ 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

Suppose that $\mathcal{R}_C$ is a product of fields. Then $\text{Res}_K^\mathbb{Q} C$ 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. [Quer-2000, Proposition 5.1, Lemma 5.3].
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**

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

**Proof.**

The proof is a modification of [Ribet-1992, Corollary 6.6]. Recall that it is given that $C$ is a $\mathbb{Q}$-curve defined over $K$ and let $A = \text{Res}^K_{\mathbb{Q}} C$. 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.
Proof con’t.

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
\[ x \otimes y \mapsto x \cdot \lambda_{\sigma^{-1}} \otimes \left( \sigma \mu_C(\sigma^{-1}) \right)^{-1} (\sigma(y)). \]
• From Proposition 4, 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 \( \hat{\rho}_{C,\beta,\pi} : G_\mathbb{Q} \to \text{GL}_2(M_\beta,\pi) \).

• 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

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

which can be simplified to the expression

\[
x \otimes y \mapsto x \cdot \beta(\sigma)^{-1} \otimes \mu_C(\sigma)(\sigma(y)).
\]
• 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 $\overline{\mathbb{Q}}^*_p \cdot \text{GL}_2(\mathbb{Q}_p)$, and it satisfies

$$\mathcal{P}\hat{\rho}_{C,\beta,\pi} |_{G_K} \cong \mathcal{P}\hat{\phi}_{C,p},$$

where $\hat{\phi}_{C,p} : G_K \to \text{GL}_2(\mathbb{Q}_p)$ 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 $\epsilon_{\beta}$ is a character and

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

(3)

where $\chi_p : G_\mathbb{Q} \to \mathbb{Z}_p^*$ is the $p$-th cyclotomic character.
• Given two splitting maps $\beta, \beta'$ for $C$, there is a character $\chi : G_\mathbb{Q} \to \overline{\mathbb{Q}}^*$ such that $\beta' = \chi \beta$.

• Conversely, if $\beta$ is a splitting map, then $\beta' = \chi \beta$ is a splitting map for any character $\chi : G_\mathbb{Q} \to \overline{\mathbb{Q}}^*$. 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 $A_\beta$. 
• 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 \( GL_2 \) type attached to \( C \). This follows because \( J_1(N) \) decomposes into product of \( A_f \)'s up to isogeny over \( \mathbb{Q} \) [Ribet-1980-twist].

• By Proposition 2, \( A_f \) 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 a 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.
• We have constructed representations

\[ \hat{\rho}_{C,\beta,\pi} : G_{\mathbb{Q}} \rightarrow \text{GL}_2(M_{\beta,\pi}) \]

attached to the \( \mathbb{Q} \)-curve \( C \).

• However, the construction depends on a choice of splitting map \( \beta : G_{\mathbb{Q}} \rightarrow \overline{\mathbb{Q}}^* \) for \( C \), which is related to picking a \( \mathbb{Q} \)-curve \( C' \) defined over \( K' \) in the \( \overline{\mathbb{Q}} \)-isomorphism class of \( C \) such that the decomposition of \( \text{Res}_{K'}^{K} E' \) up to isogeny over \( \mathbb{Q} \) is a product of non-isogenous abelian varieties of GL₂-type.

• We now explain how this is done explicitly in our example.
Let $G_{\mathbb{Q}(\sqrt{5})/\mathbb{Q}} = \{\sigma_1, \sigma_5\}$. There is a 2-isogeny $\sigma_5 C \to C$ defined over $\mathbb{Q}(\sqrt{5}, \sqrt{2})$, whence we set $\mu_C(\sigma_5)$ to be this isogeny and $\mu_C(\sigma_1) = 1$. The cocycle $c_C(\sigma, \tau) = \mu_C(\sigma)^{\sigma} \mu_C(\tau) \mu_C(\sigma \tau)^{-1}$ can also be described as arising from a cocycle $\alpha_C \in H^1(G_{\mathbb{Q}}, \overline{\mathbb{Q}}^*/\mathbb{Q}^*)$ given by $\mu_C(\sigma)^*(\omega_C) = \alpha_C(\sigma)\omega_C'$, with $\omega_C, \omega_C'$ being the invariant differentials on $C, C' = \sigma C$, through the formula

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

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,

\[ \alpha_C(\sigma_1) = 1 \]
\[ \alpha_C(\sigma_5) = \frac{1 + \sqrt{5}}{\sqrt{2}} \]

This can be computed using the discussion in [Quer-2000, p. 288]. Let \( G_{\mathbb{Q}(\sqrt{5}, \sqrt{2})/\mathbb{Q}} = \{\sigma_1, \sigma_2, \sigma_5, \sigma_{10}\} \). Then \( c_C(\sigma, \tau) \) factors through this group and has the representative values

\[ c_C(\sigma_2, \sigma_2) = 1 \]
\[ c_C(\sigma_{10}, \sigma_{10}) = 2 \]
\[ c_C(\sigma_2, \sigma_{10}) = -c_C(\sigma_{10}, \sigma_2)(= -1). \]
• It follows that $\mathcal{R}_C \cong M_2(\mathbb{Q})$ and hence $\text{Res}^\mathbb{Q}_{\sqrt{5}, \sqrt{2}} E$ 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 $\text{Res}^\mathbb{Q}_{\sqrt{5}, \sqrt{2}} E$ up to isogeny over $\mathbb{Q}$ does not include any abelian varieties of $GL_2$-type.

• The reason for this is the cocycle $c_C(\sigma, \tau)$ isn’t equal to a cocycle of the form $\beta(\sigma)\beta(\tau)\beta(\sigma \tau)^{-1}$ for a splitting map $\beta(\sigma)$ as cocycles in $B^2(G_\mathbb{Q}, \mathbb{Q}^*)$. 
Proposition

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. [Quer-2000, p. 294].
We call \( c^{\pm}(\sigma, \tau) = \text{sgn} \, c(\sigma, \tau) \) the sign component of \( c(\sigma, \tau) \).

**Proposition**

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

**Proof.**

Let \( d(\sigma) = \deg \mu_C(\sigma) \) be the degree map. In the terminology of [Quer-2000, 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 [Quer-2000, Theorem 3.1]. \( \square \)
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

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

#### Proof.

cf. [Quer-2000, Theorem 4.2].

### Proposition

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

#### Proof.

cf. [Quer-2000, p. 302].
Proposition

\[ H^2(G_{\mathbb{Q}_p}, \{\pm 1\}) \cong \{\pm 1\} \text{ for all finite primes } p. \]

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. [Serre-1968-local-fields, 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. [Vigneras-1980, Theorem 1.1]).

Proposition

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. [Quer-2000, p. 302].
The above results imply that a possible choice of splitting map $\beta$ for $E$ is given by

$$\beta(\sigma) = \sqrt{\epsilon(\sigma)} \sqrt{d(\sigma)},$$  \hspace{1cm} (4)

where $d(\sigma) = \deg \mu_{\mathbb{C}}(\sigma)$, $\epsilon = \epsilon_4 \epsilon_5$, 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 $c_C(\sigma, \tau)$ 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 $C_\beta$ defined over a number field $K_\beta$ in the $\overline{\mathbb{Q}}$-isomorphism class of $E$ such that $c_{C_\beta}(\sigma, \tau) = c_\beta(\sigma, \tau)$ as cocycles (not just as classes).

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

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

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 $\mathbb{Q}^*$. 
We wish to find a $\gamma_2$ such that

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

satisfies

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

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 $G_{K_\beta/Q} = \{\sigma_1^\pm, \sigma_5^\pm\}$. The unit group of $K_\beta$ is generated by

$$u_1 = -1$$
$$u_2 = 2 - z^2$$
$$u_3 = -z^2 + z + 2$$
$$u_4 = -z^3 + z^2 + 3z - 3$$

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 (5). 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 $\alpha_2(\sigma) = \alpha_C(\sigma) \frac{\sigma \sqrt{\gamma}}{\sqrt{\gamma}}$ 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

$$\frac{\sigma_5^+ \gamma}{\gamma} = \frac{g^2}{2},$$
$$\frac{\sigma_5^- \gamma}{\gamma} = \frac{g^2}{2} \frac{1}{u_4^2},$$
$$\frac{\sigma_1^+ \gamma}{\gamma} = 1,$$
$$\frac{\sigma_1^- \gamma}{\gamma} = u_3^2,$$
Let $C_\beta$ be the $\mathbb{Q}$-curve defined over $K_\beta$ in the $\overline{\mathbb{Q}}$-isomorphism class of $E$ given by

\[
Y^2 = X^3 - 3 \left( \frac{-5 + 3\sqrt{5}}{2} \right) \left( (3 + 2\sqrt{5})s - 3t \right) \gamma^2 X \\
+ 4\nu \left( (17 - 4\sqrt{5})s - (45 - 18\sqrt{5})t \right) \gamma^3
\]  

(6)

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

Let $\alpha_{C_\beta}(\sigma)$ be the cocycle in $H^1(G_{\mathbb{Q}}, \overline{\mathbb{Q}}^*/\mathbb{Q}^*)$ given by $\mu_{C_\beta}(\sigma)^* (\omega_{C_\beta}) = \alpha_{C_\beta}(\sigma) \omega_{C_\beta}'$, where $C_\beta' = \sigma C_\beta$. From consideration of how twisting affects the $\alpha_C(\sigma)$ [Quer-2000, p. 291], we have that

$$
\alpha_{C_\beta}(\sigma) = \alpha_C(\sigma) \frac{\sigma \sqrt{\gamma}}{\sqrt{\gamma}} = \alpha_2(\sigma).
$$
The values $\alpha_2(\sigma)$ lie in $K_\beta$. Hence, if we use $C_\beta$ instead of $E$, then $C_\beta$ is a $\mathbb{Q}$-curve defined over $K_\beta$ and we have that

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

as cocycles.

Now work of Quer [Quer-2000, Theorem 5.4, Case (2)] implies that

$$\text{Res}^K_{K_\beta} C_\beta \sim_{\mathbb{Q}} A_\beta \times A_{\beta'},$$

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 $\mathbb{Q}(\sqrt{5})$. 
Proposition

The elliptic curve $C$ has the following properties.

- **C has potentially good ordinary reduction in characteristic 3 if** $s \not\equiv 0 \pmod{3}$ and potentially good supersingular reduction in characteristic 3 if $s \equiv 0 \pmod{3}$.

- **The sign component**
  
  $$c_{C}^\pm(\sigma, \tau) = \text{sgn} \mu_{C}(\sigma) \sigma \mu_{C}(\tau) \mu_{C}(\sigma \tau)^{-1} \in H^2(G_{\mathbb{Q}}, \{\pm 1\})$$

  is trivial when restricted to $G_{\mathbb{Q}_3}$.

Proof.

Note $s^2 - 10st + 5t^2 \not\equiv 0 \pmod{3}$. The elliptic curve $C$ has potentially good reduction because the denominator of its $j$-invariant is not divisible by a prime above 3 by Equation (1). Its $j$-invariant is zero in characteristic 3 if and only if $s \equiv 0 \pmod{3}$ so $C$ is supersingular in characteristic 3 if and only if $s \equiv 0 \pmod{3}$. Since the sign component $c_{C}^\pm(\sigma, \tau)$ is given by the quaternion algebra $(5, 2)$ by Proposition 6, we see that it is trivial when restricted to $G_{\mathbb{Q}_3}$. 
Theorem
The abelian varieties $A_{\beta}$ and $A_{\beta'}$ are modular.

Proof.
In the case of potentially good ordinary reduction, $C$ satisfies the hypotheses of [Ellenberg-2001, Theorem 5.1] because of Proposition 11 so we deduce that it is modular. In the case of potentially good supersingular reduction, we note that $\mathbb{P}\rho_{C,\beta,\pi}$ is unramified at 3 so by [Ellenberg-2001, Theorem 5.2] we also deduce that $C$ is modular.

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

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

Proof.

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

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

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

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

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


J. Buhler and B. Gross.
Arithmetic on elliptic curves with complex multiplication II.

I. Chen.
On the equation $a^2 + b^{2p} = c^5$, 39 pages.
May 2008.

J. Ellenberg and C. Skinner.
On the modularity of $\mathbb{Q}$-curves.

J. Ellenberg.
Galois representations attached to $\mathbb{Q}$-curves and the generalized Fermat equation $A^4 + B^2 = C^p$.

J. Ellenberg and C. Skinner.
On the modularity of $\mathbb{Q}$-curves.
B. Gross.

*Arithmetic on Elliptic Curves with Complex Multiplication.*
Number 776 in Lecture Notes in Mathematics. Springer-Verlag, 1980.

H. Montgomery and P. Weinberger.

Notes on small class numbers.

J. Quer.

$\mathbb{Q}$-curves and abelian varieties of $GL_2$-type.

K. Ribet.

Twists of modular forms and endomorphisms of abelian varieties.

K. Ribet.

Abelian varieties over $\mathbb{Q}$ and modular forms.

**J.-P. Serre.**

*Corps locaux.*


**J.-P. Serre.**


**H. Stark.**


**M.-F. Vigneras.**

*Arithmétique de algèbres de quaternions.*

Number 800 in Lecture notes in mathematics. Springer-Verlag, 1980.