Diagonal Quotient Surfaces
and a Question of Mazur

Introduction
Let $E/K$ be an elliptic curve over a number field $K$, $N$ an odd prime,

$$\bar{\rho}_{E/K,N} : G_K \rightarrow Aut(E[N]) \simeq GL_2(\mathbb{Z}/N\mathbb{Z})$$

its associated Galois representation modulo $N$.

Question: To what extent is the isogeny class of $E/K$ determined by the isomorphism class of $\bar{\rho}_{E/K,N}$?

Note: By definition, $\bar{\rho}_{E/K,N} \simeq \bar{\rho}_{E'/K,N} \Leftrightarrow \exists G_K$-isomorphism $\psi : E[N] \sim \rightarrow E'[N]$.

Mazur (1978): $\exists ? E$ and $E'/Q$ with $E \not\sim E'$ such that $\bar{\rho}_{E/K,N} \simeq \bar{\rho}_{E'/K,N}$ for some $N \geq 7$?


Halberstadt-Kraus (1996): $\exists \ \infty'$ly many examples for $N = 7$. 
Conjecture 1 (Frey, 1988): \( \exists \) a constant \( M_{E,K} \) s. th.
\[ S_{N,E}(K) \overset{\text{def}}{=} \{ E'/K : \bar{\rho}_{E'/K,N} \simeq \bar{\rho}_{E/K,N}, E' \not\sim E \}/\sim = \phi, \quad \text{for } N \geq M_{E,K}. \]

Note: Faltings’ Theorem (Mordell Conjecture) \( \Rightarrow \)
\[ \#S_{N,E}(K) < \infty \text{ for all } N \geq 7. \]

Theorem 0 (Frey, 1996): For \( K = \mathbb{Q} \), Conjecture 1 is equivalent to the Asymptotic Fermat Conjecture:

\textbf{(AFC)} For every \( a, b, c \in \mathbb{Z}, abc \neq 0 \), the set
\[ F_{a,b,c} = \bigcup_{n \geq 4} \{ (x_n, y_n, z_n) \in \mathbb{Z}^3 : ax_n^3 + by_n^3 = cz_n^3, \]
\[ (x_n, y_n, z_n) = 1 \} \]
is finite.

Conjecture 2 (Darmon, 1994): \( \exists \) constant \( M_K \) s. th.
\[ S_N(K) := \bigcup_{E/K} S_{N,E}(K) = \phi, \quad \forall N \geq M_K. \]

Conjecture 3 (Darmon, 1994): \( \exists \) constant \( M \) s. th.
\[ \#S_N(K) < \infty, \quad \forall N \geq M. \]

Conjecture 3': Conjecture 3 is true for \( M = 23 \).
Note: We can alternately define the set $\mathcal{S}_N(K)$ as
$$\mathcal{S}_N(K) = \{(E, E')/K : E \not\sim E' \text{ and } \exists G_K\text{-isom. } \psi : E[N] \simeq E'[N] \}/\simeq.$$ 

Definition: A $G_K$-isomorphism $\psi : E[N] \simeq E'[N]$ is called trivial if it is “induced by an isogeny of very small degree”, i.e. there exists a cyclic isogeny $f : E \rightarrow E'$ with $\deg(f) \leq 27, (\neq 22, 23, 26)$ s. th.
$$\psi = k \cdot f|_{E[N]}, \text{ for some } k, (k, N) = 1.$$ 

Conjecture 4: The set
$$\mathcal{S}^*_N(K) = \{(E, E')/K : \exists \text{ non-trivial } G_K\text{-isom. } \psi : E[N] \simeq E'[N] \}/\simeq.$$ 

is finite, for all $N \geq 23.$

Remarks. 1) Clearly, Conjecture 4 $\Rightarrow$ Conjecture $3'$ (because $\mathcal{S}^*_N(K) \supset \mathcal{S}_N(K)$).

2) On the other hand, the set
$$\mathcal{T}_N(K) = \{(E, E')/K : \exists \text{ trivial } G_K\text{-isom. } \psi : E[N] \simeq E'[N] \}/\simeq.$$ 

is always infinite!
1. Diagonal Quotient Surfaces

Given: $X$ a (smooth, projective) curve over $K$
$G \leq Aut(X)$ a group of auto’s of $X/K$
$\alpha \in Aut(G)$ an automorphism of $G$

Let: $Y = X \times X$ denote the product surface
$\Delta_\alpha = \{(g, \alpha(g)) : g \in G\} \leq G \times G$
– the “twisted diagonal subgroup”
$Z = Z_{X,G,\alpha}$ the diagonal quotient surface
$\sigma : \tilde{Z} \to Z$ its desingularization

**Proposition 1:** The functor $Z_{N,\varepsilon}$, defined by

$$Z_{N,\varepsilon}(K) = \{(E, E', \psi)/_K : \psi : E[N] \sim \to E'[N],$$
$$\det(\psi) = \varepsilon\}/\simeq$$

is (coarsely) representable by an open subscheme $Z'_{N,\varepsilon}$
of the diagonal quotient surface (“modular diagonal quotient surface”)

$$Z_{N,\varepsilon} := Z_{X,G_N,\alpha_\varepsilon},$$

where $X = X(N)$ is the modular curve of level $N$,
$G_N = SL_2(\mathbb{Z}/N\mathbb{Z})/\{\pm 1\}$,
$\alpha_\varepsilon : g \mapsto Q_\varepsilon g Q_\varepsilon^{-1}$, with $Q_\varepsilon = \begin{pmatrix} \varepsilon & 0 \\ 0 & 1 \end{pmatrix}$.
**Remarks. 1)** $Z_{N,\varepsilon}$ may be viewed as a “degenerate Hilbert modular surface” of discriminant $\Delta = N^2$. (point of view of C.F. Hermann)

2) Just like the curves $X(N)$, the surfaces $Z_{N,\varepsilon}$ have canonical models defined over $\mathbb{Q}$, and the quotient maps

$$X(N) \times X(N) \xrightarrow{\varphi} Z_{N,\varepsilon} \xrightarrow{\psi} X(1) \times X(1)$$

are also $\mathbb{Q}$-rational (even though the elements of $G_N$ are only defined over $\mathbb{Q}(\zeta_N)^+$).

Thus, the classification of iso.’s between the $\bar{\rho}_{E/K,N}$’s $\leftrightarrow$ the study of rational points on $Z_{N,\varepsilon}$:

$$Z_{N,\varepsilon}(K)^{\text{ “”}} = \mathbb{T}_{N,\varepsilon}(K) \cup S_{N,\varepsilon}^*(K) \cup \text{cusps}_{N,\varepsilon}(K)$$

Theorem 1 (C.F. Hermann; K.-Schanz): The rough classification type of $\tilde{Z}_{N,\varepsilon}$ is completely determined by its geometric genus $p_g = p_g(\tilde{Z}_{N,\varepsilon})$; in particular, its Kodaira dimension is

$$\kappa(\tilde{Z}_{N,\varepsilon}) = \min(p_g - 1, 2)$$

Corollary: $\tilde{Z}_{N,\varepsilon}$ is of general type $\forall \varepsilon \iff N \geq 13$. 
2. Modular DQS’s and Conjecture 4

**Need:** a geometric interpretation of the condition “\( \psi \) is induced by an isogeny”.

\[ \rightarrow \text{Hecke correspondences } T_n \text{ on } X(N) \]

\[ \begin{array}{ccc}
T_n & \sim & T_n \subset Y = X(N) \times X(N) \\
X(N) & \downarrow & X(N) \\
X_0(n) & \downarrow & \Delta\varepsilon \\
X(1) & \downarrow & \bar{T}_{n,k} \subset Z = \Delta\varepsilon \setminus Y
\end{array} \]

**Note:** \( T_{n,k} \) is \( \Delta\varepsilon \)-invariant \( \iff \) \( k^2n\varepsilon \equiv 1 \pmod{N} \).

**Proposition 2:** The set \( \mathbb{T}_{N,\varepsilon} \) has the following geometric interpretation:

\[ \mathbb{T}_{N,\varepsilon}(K) = \bigcup_{n,k} \bar{T}_{n,k}(K) \setminus \text{cusps}(K) \]

In addition, we have

\[ g(\bar{T}_{n,k}) \leq 1 \iff \begin{cases} n \leq 27, n \neq 22, 23, 26 \\ k^2n\varepsilon \equiv 1 \pmod{N} \end{cases} \]
Remark. Thus we have:

\[ Z_{N,\varepsilon}(K) = T_{N,\varepsilon}(K) \cup S^*_{N,\varepsilon}(K) \cup \text{cusps}(K) \]

infinite \cup finite for \( N \geq 13 \)

Conjecture 5: If \( N \geq 23 \), then every curve \( C \) on \( Z_{N,\varepsilon} \) of genus \( g(C) \leq 1 \) is modular,
i.e. \( C = \overline{T_{n,k}} \), for some \( n, k \).

Remark. Conj. 4 \( \Rightarrow \) Conj. 5

\( \Leftarrow \) via Lang’s Conjecture

Lang’s Conjecture: If \( Z \) is a surface of general type and

\[ Z_{exc} = \bigcup_{C \subset Z, g(C) \leq 1} C, \]

then a) \( Z_{exc} \) consists of finitely many curves;
b) the open variety \( Z \setminus Z_{exc} \) is Mordellic.

Remark. Conjecture 5 \( \Rightarrow \) Lang’s Conjecture, part a) for \( Z_{N,\varepsilon} \).
3. Evidence for Conjecture 5

a) $G_N$-equivariant curves:

Proposition 3. If $N \geq 23$, then

a) $H \leq G_N \Rightarrow g(H \setminus X(N)) \geq 2$.

b) Every curve $C$ on $Z_{N,\epsilon}$ with $g(C) \leq 1$ lifts to a $\Delta_\epsilon$-equivariant curve $\tilde{C}$ on $Y = X(N) \times X(N)$:

\[
\begin{array}{c}
\tilde{C} \\
\downarrow \quad \downarrow \\
X(N) \quad X(N) \\
\downarrow G_N \quad \downarrow G_N \\
X(1) \quad X(1)
\end{array}
\]

However: $\exists \infty$'ly many $\Delta_\epsilon$-equivariant curves $C$ on $Z_{N,\epsilon}$ with sufficiently large genus $g(C) \gg 0$. 
b) Minimal models:

**Conjecture 6:** (Hermann, 1991) If \( N \geq 7 \), then the minimal model \( \tilde{Z}_{N,\varepsilon}^{\text{min}} \) of \( \tilde{Z}_{N,\varepsilon} \) is obtained by blowing down “known curves”.

**Remarks.**
1) Conj. 5 \( \Rightarrow \) Conjecture 6 (for \( N \geq 23 \)).
2) Conjecture 6 \( \Leftrightarrow \) explicit formula for \( P_2(\tilde{Z}^{\text{min}}) \)
   \( \Leftrightarrow \) explicit formula for \( K^2_{\tilde{Z}^{\text{min}}} \).

In particular: Conject. 6 \( \Rightarrow \) \( K^2_{\tilde{Z}^{\text{min}}} - K^2_{\tilde{Z}} \leq 6 \).

(Note: Vanishing thms \( \Rightarrow \) \( K^2_{\tilde{Z}^{\text{min}}} - K^2_{\tilde{Z}} \leq f(N) \),
where \( f(N) \) is a quadratic polynomial in \( N \).)

3) Conjecture 6 is a natural analogue of a Conjecture of Hirzebruch for Hilbert modular surfaces; this latter conjecture was proven by C.F. Hermann in 1987 in many cases. His method also yields:

**Theorem 2** (Hermann) If \( N \equiv 7 \pmod{8} \) and \( \varepsilon \equiv -1 \pmod{N} \), then Conjecture 6 is true.

**Theorem 3:** Conjecture 6 is true for \( N \leq 13 \).