

Mazur's Question on Mod N Galois Representations

Introduction

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

$\bar{\rho}_{E/K,N} : G_K \rightarrow \text{Aut}(E[N]) \simeq \text{GL}_2(\mathbb{Z}/N\mathbb{Z})$
its associated Galois representation modulo N .

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

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

Kraus-Oesterlé (1992): Yes! (for $N = 7$).

Frey + group (~ 1993): Computer search: lots of
examples for $N = 7, 11$.

Halberstadt-Kraus (1997): \exists ∞ 'ly many exam-
ples for $N = 7$.

K.-Rizzo (1999): \exists ∞ 'ly many families of examples
for $N = 11$.

Note: Faltings' Theorem (=Mordell Conjecture) \Rightarrow

$\mathbb{S}_{N,E}(K) \stackrel{\text{def}}{=} \{E'/K : \bar{\rho}_{E'/K,N} \simeq \bar{\rho}_{E/K,N},\} / \simeq$
is finite, for all $N \geq 7$.

Conjecture 1 (Frey, 1988): \exists a constant $M_{E,K}$ s. th.

$\mathbb{S}'_{N,E}(K) := \{E' \in \mathbb{S}_{N,E}(K) : E' \not\sim E\} = \emptyset,$
for $N \geq M_{E,K}$.

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

(AFC) For every $a, b, c \in \mathbb{Z}, abc \neq 0$, the set

$$F_{a,b,c} = \bigcup_{n \geq 4} \{(x_n, y_n, z_n) \in \mathbb{Z}^3 : ax_n^n + by_n^n = cz_n^n, \\ (x_n, y_n, z_n) = 1\}$$

is finite.

Conjecture 2 (Darmon, 1994): \exists constant M_K s. th.

$$\mathbb{S}'_N(K) := \bigcup_{E/K} \mathbb{S}'_{N,E}(K) = \emptyset, \quad \forall N \geq M_K.$$

Conjecture 3 (Darmon, 1994): \exists constant M s. th.

$$\#(\mathbb{S}'_N(K)/\text{twists}) < \infty, \quad \forall N \geq M.$$

Conjecture 3': Conjecture 3 is true for $M = 23$.

Note: We can alternately define the set $\mathcal{S}'_N(K)$ as

$$\mathcal{S}'_N(K) = \{(E, E')/_K : E \not\sim E' \text{ and } \exists G_K\text{-isom.} \\ \psi : E[N] \xrightarrow{\sim} E'[N]\} / \simeq .$$

Definition: A G_K -isomorphism $\psi : E[N] \xrightarrow{\sim} E'[N]$ 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.

$$\psi = k \cdot f|_{E[N]}, \quad \text{for some } k, (k, N) = 1.$$

Conjecture 4: The set

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

is **finite modulo twists**, 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

$$\mathcal{T}_N(K) = \{(E, E')/_K : \exists \text{trivial } G_K\text{-isom.} \\ \psi : E[N] \xrightarrow{\sim} E'[N]\} / \simeq .$$

is always **infinite!**

1. The Functor \mathcal{Z}_N

The assignment $K \mapsto \mathcal{Z}_N(K)$, where

$$\mathcal{Z}_N(K) = \{(E, E', \psi)_{/K} : \psi : E[N] \xrightarrow{\sim} E'[N]\} / \simeq,$$

naturally extends to a **functor** $\mathcal{Z}_N : \text{Sch}/\mathbb{Q} \rightarrow \text{Sets}$.

We have a natural decomposition (of functors)

$$\mathcal{Z}_N(K) = \coprod_{\varepsilon \in (\mathbb{Z}/N\mathbb{Z})^\times} \mathcal{Z}_{N,\varepsilon}(K),$$

where

$$\mathcal{Z}_{N,\varepsilon}(K) = \{(E, E', \psi) \in \mathcal{Z}_N(K) : \det(\psi) = \varepsilon\};$$

here, the **determinant** of ψ is defined by

$$e_N^{E'}(\psi(P), \psi(Q)) = e_N^E(P, Q)^{\det(\psi)}, \forall P, Q \in E[N].$$

Proposition 1: The functors \mathcal{Z}_N and $\mathcal{Z}_{N,\varepsilon}$ are **coarsely representable** by normal affine surfaces Z_N and $Z_{N,\varepsilon}$ over \mathbb{Q} . Moreover, the surfaces $Z_{N,\varepsilon}$ are the connected components of Z_N , and each $Z_{N,\varepsilon}$ is geometrically connected.

Proposition 2: The representation map

$$r_{N,K} : \mathcal{Z}_N(K) \rightarrow Z_N(K)$$

is **surjective**, and is **injective** up to **simultaneous twists**.

Remarks: 1) Thus, the classification of isomorphisms between the $\bar{\rho}_{E/K,N}$'s is essentially the same as the study of rational points on the surfaces $Z_{N,\varepsilon}$.

2) By considering (as in Deligne/Rapoport) generalized elliptic curves (for which the order of the Néron polygon is divisible by N), we can define a compactification \bar{Z}_N (resp. $\bar{Z}_{N,\varepsilon}$) of the above moduli functors. These are then coarsely represented by projective normal surfaces \bar{Z}_N and $\bar{Z}_{N,\varepsilon}$.

3) Let $X(N)_{/\mathbb{Q}}$ denote Shimura's canonical model/ \mathbb{Q} of the modular curve $X(N)_{/\mathbb{C}} = \Gamma(N) \backslash \mathbb{H}^*$. Then we have natural (\mathbb{Q} -rational) morphisms

$$X(N)_{/\mathbb{Q}} \times X(N)_{/\mathbb{Q}} \xrightarrow{\varphi} \bar{Z}_{N,\varepsilon} \xrightarrow{\psi} X(1)_{/\mathbb{Q}} \times X(1)_{/\mathbb{Q}}.$$

Moreover, both are finite covering maps of degree

$$\deg(\varphi) = \deg(\psi) = \frac{1}{2} |\mathrm{SL}_2(\mathbb{Z}/N\mathbb{Z})|.$$

2. The Geometry of Z_N

Let $X(N)$ denote the modular curve/ \mathbb{C} of level N ,

$$Y(N) = X(N) \setminus \{\text{cusps}\},$$

$$G_N = \text{SL}_2(\mathbb{Z}/N\mathbb{Z})/\{\pm 1\},$$

$\alpha_\varepsilon \in \text{Aut}(G_N)$ be defined by

$$\alpha_\varepsilon : g \mapsto Q_\varepsilon g Q_\varepsilon^{-1}, \text{ where } Q_\varepsilon = \begin{pmatrix} \varepsilon & 0 \\ 0 & 1 \end{pmatrix}.$$

Proposition 3: We have

$$Z_{N,\varepsilon} \otimes \mathbb{C} = \Delta_\varepsilon \setminus (Y(N) \times Y(N)),$$

$$\bar{Z}_{N,\varepsilon} \otimes \mathbb{C} = \Delta_\varepsilon \setminus (X(N) \times X(N))$$

where $\Delta_\varepsilon = \{(g, \alpha_\varepsilon(g)) : g \in G_N\} \leq G_N \times G_N$.

Thus, $Z_{N,\varepsilon}$ (and $\bar{Z}_{N,\varepsilon}$) may be called a modular diagonal quotient surface.

Remarks: 1) $\bar{Z}_{N,\varepsilon} \otimes \mathbb{C}$ may also be viewed as a “degenerate Hilbert modular surface” of discriminant $\Delta = N^2$. (Point of view of C.F. Hermann)

2) Each surface $\bar{Z}_{N,\varepsilon} \otimes \mathbb{C}$ has a finite number of (isolated) cyclic quotient singularities. We let $\tilde{Z}_{N,\varepsilon}$ denote the minimal desingularization.

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 $\forall \varepsilon \Leftrightarrow N \geq 13$.

Remark: We also have:

The surface $\tilde{Z}_{7,1}$ is rational \rightarrow Halberstadt-Kraus.

The surface $\tilde{Z}_{11,1}$ is elliptic \rightarrow K.-Rizzo.

3. Hecke Curves on Z_N and Conjecture 4

Need: a geometric interpretation of the condition “ ψ is induced by an isogeny”.

Recall: The modular curve $Y_0(n) = X_0(n) \setminus \{\text{cusps}\}$ coarsely represents the functor

$$K \rightarrow \mathcal{Y}_0(n)(K) = \{(E, E', f)_{/K} : E \xrightarrow{f} E' \text{ cyclic,} \\ \deg(f) = n\}.$$

Thus, if n, k satisfy $(nk, N) = 1$, then the rule

$$(E, E', f) \mapsto (E, E', (kf)|_{E[N]})$$

defines a morphism of functors and of varieties:

$$\tau_{n,k} : \mathcal{Y}_0(n) \rightarrow \mathcal{Z}_N \text{ and } \tau_{n,k} : X_0(n) \rightarrow \bar{Z}_N.$$

We call the image $\bar{T}_{n,k} = \text{Im}(\tau_{n,k}) \subset \bar{Z}_{N,\varepsilon}$ a **Hecke curve**; here $\varepsilon \equiv nk^2 \pmod{N}$.

Remarks: 1) The map $\tau_{n,k} : X_0(n) \rightarrow \bar{T}_{n,k}$ is finite and **birational**. If $\tilde{T}_{n,k}$ denotes the total transform of $\bar{T}_{n,k}$ on $\tilde{Z}_{N,\varepsilon}$, then $\tilde{T}_{n,k}$ has **ordinary singularities** on $\tilde{Z}_{N,\varepsilon} \setminus \{\text{cuspidal curves}\}$, and singularities of type $x^a = y^b$ “at infinity”.

2) In the finite part, the curves $\tilde{T}_{n,k}$ intersect only at **CM-points** (=generalization of **Heegner points**), and their intersection multiplicity can be computed in terms of **representation numbers of binary quadratic forms**.

3) As the name suggests, the $\tilde{T}_{n,k}$'s are closely connected to the **Hecke correspondences** T_n on $X(N)$:

$$\begin{array}{ccc}
 & T_n & \rightsquigarrow T_n \subset Y = X(N) \times X(N) \\
 p_n \swarrow & \downarrow & \searrow p_n \circ w_n \\
 X(N) & & X(N) \rightsquigarrow T_{n,k} = (\langle k \rangle \times id)T_n \subset Y \\
 \downarrow & X_0(n) & \downarrow \Delta_\varepsilon \\
 X(1) & & X(1) \quad \bar{T}_{n,k} \subset Z = \Delta_\varepsilon \setminus Y
 \end{array}$$

4) Thus, the set $\mathbb{T}_{N,\varepsilon}$ has the following **geometric interpretation**:

$$\mathbb{T}_{N,\varepsilon}(K) = \bigcup_{\substack{n,k \\ g(\bar{T}_{n,k}) \leq 1}} \bar{T}_{n,k}(K) \setminus \text{cusps}(K)$$

In addition, we have

$$g(\bar{T}_{n,k}) \leq 1 \iff n \leq 27, n \neq 22, 23, 26.$$

Note: Thus we have:

$$\bar{Z}_{N,\varepsilon}(K) = \underbrace{\mathbb{T}_{N,\varepsilon}(K)}_{\text{infinite}} \cup \mathbb{S}_{N,\varepsilon}^*(K) \cup \underbrace{\text{cusps}(K)}_{\text{finite for } N \geq 13}$$

Conjecture 5: If $N \geq 23$, then every curve C on $\bar{Z}_{N,\varepsilon}$ of genus $g(C) \leq 1$ is **modular**, i.e. $C = \bar{T}_{n,k}$, 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

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

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 $\bar{Z}_{N,\varepsilon}$.

4. Evidence for Conjecture 5

a) G_N -equivariant curves:

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

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

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

$$\begin{array}{ccc} & \tilde{C} & \\ & \swarrow \quad \searrow & \\ X(N) & \downarrow & X(N) \\ \downarrow^{G_N} & C & \downarrow^{G_N} \\ X(1) & & X(1) \end{array}$$

However: \exists ∞ 'ly many Δ_ε -equivariant curves C on $Z_{N,\varepsilon}$ with sufficiently large genus $g(C) \gg 0$.

b) Minimal models:

Conjecture 6: (Hermann, 1991) If $N \geq 7$, then the minimal model $\tilde{Z}_{N,\varepsilon}^{min}$ 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 $P_2(\tilde{Z}^{min})$
 \Leftrightarrow explicit formula for $K_{\tilde{Z}^{min}}^2$.

In particular: Conject. 6 $\Rightarrow K_{\tilde{Z}^{min}}^2 - K_{\tilde{Z}}^2 \leq 6$.

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

3) Conjecture 6 is a natural analogue of a Conjecture of Hirzebruch/Zagier 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 $N \leq 13$.

5. Hecke Curves and CM-Points

CM-Points: these are points of the form

$$P = (E, E', h|_{E[N]}),$$

where E has **CM** and $0 \neq h \in \text{Hom}(E, E') \simeq \mathbb{Z}^2$.

Notes: 1) Each **CM-point** P defines a **positive definite binary quadratic form** $q = q_{E, E'} = \deg|_{\text{Hom}(E, E')}$.
2) Given a positive definite binary quadratic form q , **there exist finitely many** pairs (E, E') with

$$q_{E, E'} \sim q.$$

The number $c_q > 0$ of such pairs is given by an **explicit formula**.

3) A **CM-point** P need **not** be **rational** over \mathbb{Q} ; its precise field of definition can be determined (by **class field theory**).

Fact: Distinct **Hecke curves** meet only at **cusps** and at **CM-points**.

Local Intersection Numbers of Hecke curves:

Let $\mathcal{R}_q(n)$ be the set of primitive representations of n by q , i.e.,

$$\mathcal{R}_q(n) = \{(x, y) \in \mathbb{Z}^2 : q(x, y) = n, \gcd(x, y) = 1\},$$

and put

$$\begin{aligned} r_q(n, k, n', k'; N) \\ = \#\{\vec{v} \times \vec{v}' \in \mathcal{R}_n \times \mathcal{R}_{n'} : k\vec{v} \equiv k'\vec{v}' \pmod{N}\}. \end{aligned}$$

Then the local intersection number (at the CM-points associated to (E, E')) is

$$\begin{aligned} (T_{n,k} \cdot T_{n',k'})_{(E,E')} &:= \sum_{\psi} (T_{n,k} \cdot T_{n',k'})_{(E,E',\psi)} \\ &= \frac{1}{e_q} r_q(n, k, n', k'; N), \end{aligned}$$

where $q = q_{E,E'}$ and $e_q = |\text{Aut}(q)|$.

Thus we have

$$(T_{n,k} \cdot T_{n',k'})_{fin} = \sum_q \frac{c_q}{e_q} r_q(n, k, n', k'; N).$$

6. The case $N = 11$

Theorem 4 (K. - Rizzo) Let Z_{min} denote the minimal model of (the desingularization of) the modular diagonal quotient surface $\bar{Z} = (\bar{Z}_{11,1})/\mathbb{Q}$. Then the **canonical map** defines an elliptic fibration

$$f_{can} : Z_{min} \rightarrow \mathbb{P}_{\mathbb{Q}}^1$$

which has an **infinite number** of sections

$$S_i : \mathbb{P}_{\mathbb{Q}}^1 \rightarrow Z_{min}.$$

Notes: 1) The surface Z_{min} is obtained from the minimal desingularization \tilde{Z} of \bar{Z} by blowing down 5 (explicit) curves (cf. K.-Schanz).

2) The **sections** S_i are constructed as follows. We start with two **explicit** sections S_0 and S_1 of f_{can} which arise as components of the desingularization curves of the quotient singularities at the cusps of \bar{Z} . Since these **meet** on Z_{min} , S_1 defines a point of **infinite order** on the associated **elliptic curve** (taking S_0 as the origin), and so the i -th multiples S_i of S_1 define infinitely many distinct sections of f_{can} .

Corollary. There exist infinitely many one-parameter families of (isomorphism classes of) pairs (E, E') of non-isogenous elliptic curves E, E' defined over \mathbb{Q} whose associated Galois representations mod 11 are symplectically isomorphic:

$$\bar{\rho}_{E/\mathbb{Q},11} \simeq \bar{\rho}_{E'/\mathbb{Q},11}.$$

Notes: 1) By a one-parameter family of such pairs (E, E') we mean that the associated j -invariants of E and E' depend rationally on a parameter $t \in \mathbb{Q}$.

2) If we replace the 11 of the above theorem by any $N \geq 13$, then the resulting statement is expected to be false.

Curves on the Surface $\tilde{Z}_{11,1}$

