

# Mazur's Question and Modular Diagonal Quotient Surfaces

## 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 ( $\sim 1993$ ):** Computer search: lots of  
 examples for  $N = 7, 11$ .

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

**K.-Rizzo (1999):**  $\exists$   $\infty$ '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. [Wiles(1993):  $\#F_{1,1,1} = 10$ .]

**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  $M = 23$ , provided we restrict attention to **prime**  $N$ 's.

**Refinement:** Let's write  $E \approx E'$  if there exists a cyclic isogeny  $f : E \rightarrow E'$  with  $\deg(f) \leq 27$  (and  $\deg(f) \neq 22, 23, 26$ ).

**Conjecture 4:** For any number field  $K$ , the set

$$\mathbb{S}_N^*(K) := \{(E, E') : E \in \mathbb{S}_{N, E'}(K), E \not\approx E'\} / \simeq$$

is finite modulo twists, for all primes  $N \geq 23$ .

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

★ ★ ★ ★ ★

## Aims of this talk:

- 1) To explain the above conjectures (and counterexamples) in terms of the underlying geometrical objects (modular curves and surfaces).
- 2) To study related conjectures concerning the geometry of these objects.

# 1. Geometric Interpretations

## (a) Special Case: $E/K$ fixed

**Notation:** For  $E/K$  and  $N \geq 1$ , let

$$\tilde{\mathcal{S}}_{N,E}(K) = \{(E', \psi) : E' \in \mathcal{S}_{N,E}(K)\} / \simeq$$

where  $\psi : \bar{\rho}_{E/K,N} \xrightarrow{\sim} \bar{\rho}_{E'/K,N}$ .

**Theorem 1.** If  $N \geq 3$ , then there is an **affine smooth curve**  $X_{E/K,N}$  over  $K$  which **parametrizes** the sets  $\{\tilde{\mathcal{S}}_{N,E}(K')\}_{K'/K}$ , i.e. there are natural bijections

$$\tilde{\mathcal{S}}_{N,E}(K') \xrightarrow{\sim} X_{E/K,N}(K'), \quad \forall K'/K.$$

Moreover,  $X_{E/K,N}$  consists of  $\phi(N)$  **irreducible components**  $\{X_{E/K,N,\varepsilon}\}_{\varepsilon \in (\mathbb{Z}/N\mathbb{Z})^\times}$ , and we have

$$X_{E/K,N,\varepsilon} \otimes \mathbb{C} \simeq X'(N) = \Gamma(N) \backslash \mathfrak{H},$$

where  $\Gamma(N) = \text{Ker}(\text{SL}_2(\mathbb{Z}) \rightarrow \text{SL}_2(\mathbb{Z}/N\mathbb{Z}))$ .

**Remarks 1)** This result is **well-known** and can be proved by the methods of **Katz/Mazur's** book.

**2)** The curve  $X_{E/K,N,\varepsilon}$  classifies pairs  $(E', \psi)$  with  $\det(\psi) = \varepsilon$ , i.e.  $\psi : E[N] \xrightarrow{\sim} E'[N]$  satisfies

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

## (b) General Case

**Notation:** For  $K/\mathbb{Q}$  and  $N \geq 1$ , let

$$\tilde{\mathcal{S}}_N(K) = \{(E, E', \psi) : E' \in \mathcal{S}_{N,E}(K)\} / \simeq.$$

**Theorem 2.** If  $N \geq 3$ , then there is an **affine normal surface**  $Z_N$  over  $\mathbb{Q}$  which **coarsely parametrizes** the sets  $\{\tilde{\mathcal{S}}_N(K)\}_{K/\mathbb{Q}}$ , i.e. there are maps

$$\tilde{\mathcal{S}}_N(K) \rightarrow Z_N(K), \quad \forall K/\mathbb{Q},$$

which are injective modulo (simultaneous) twists.

Moreover,  $Z_N$  consists of  $\phi(N)$  **irreducible components**  $\{Z_{N,\varepsilon}\}_{\varepsilon \in (\mathbb{Z}/N\mathbb{Z})^\times}$ , and we have

$$Z_{N,\varepsilon} \otimes \mathbb{C} \simeq \tilde{\Delta}_{N,\varepsilon} \setminus (\mathfrak{H} \times \mathfrak{H}),$$

where  $\Gamma(N) \times \Gamma(N) \leq \tilde{\Delta}_{N,\varepsilon} \leq \mathrm{SL}_2(\mathbb{Z}) \times \mathrm{SL}_2(\mathbb{Z})$ ,

**Remarks 1)** This can be proved by an **extension** of the methods of **Katz/Mazur's** book.

**2)** The irreducible surface  $Z_{N,\varepsilon}$  (coarsely) classifies triples  $(E, E', \psi)$  with  $\det(\psi) = \varepsilon$ .

**3)** In general,  $Z_{N,\varepsilon} \otimes \mathbb{C} \not\cong Z_{N,\varepsilon'} \otimes \mathbb{C}$  unless  $\varepsilon \equiv \varepsilon' x^2 \pmod{N}$ , for some  $x \in \mathbb{Z}$ .

**4)** Clearly,  $Z_{N,\varepsilon} \otimes \mathbb{C}$  is the (finite) quotient

$$\Phi : X'(N) \times X'(N) \rightarrow Z_{N,\varepsilon} \otimes \mathbb{C}$$

by the group  $\Delta_{N,\varepsilon} = \tilde{\Delta}_{N,\varepsilon}/(\Gamma(N) \times \Gamma(N))$ . Explicitly,  $\Delta_{N,\varepsilon}$  is the “twisted” **diagonal subgroup**

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

of  $G_N = \mathrm{SL}_2(\mathbb{Z}/N\mathbb{Z})$ . Here  $\alpha_\varepsilon \in \mathrm{Aut}(G_N)$  is defined by  $\alpha_\varepsilon : g \mapsto Q_\varepsilon g Q_\varepsilon^{-1}$ , where  $Q_\varepsilon = \begin{pmatrix} \varepsilon & 0 \\ 0 & 1 \end{pmatrix}$ .

Thus,  $Z_{N,\varepsilon} \otimes \mathbb{C}$  (and  $Z_{N,\varepsilon}$ ) may be called a **modular diagonal quotient surface**.

**5)** The (affine) surface  $Z_{N,\varepsilon} \otimes \mathbb{C}$  has a natural **compactification**

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

where  $X(N)_{/\mathbb{C}} = \Gamma(N) \backslash \mathfrak{H}^*$  is the usual **modular curve** of level  $N$ .

**6)** Let  $X(N)_{/\mathbb{Q}}$  denote **Shimura’s canonical model** of  $X(N)$ . Then the above quotient map descends uniquely to a morphism

$$\bar{\Phi}_{\mathbb{Q}} : X(N)_{/\mathbb{Q}} \times X(N)_{/\mathbb{Q}} \rightarrow \bar{Z}_{N,\varepsilon} \supset Z_{N,\varepsilon}.$$

## 2. The Geometry of $Z_{N,\varepsilon}$

**Notation.** Let  $\tilde{Z}_{N,\varepsilon}$  denote the **minimal desingularization** of the surface  $\bar{Z}_{N,\varepsilon} \otimes \mathbb{C}$  (which has a finite number of (isolated) **cyclic quotient singularities**.)

**Theorem 3** (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

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

**Remark.** In his paper, **C.F. Hermann** calls the surface  $\bar{Z}_{N,\varepsilon} \otimes \mathbb{C}$  a “**degenerate Hilbert modular surface**” of discriminant  $\Delta = N^2$ .

**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**.

Since such surfaces have (in general) many rational points, one can expect **many counterexamples** to **Mazur’s question** for these values of  $N$ .

### 3. Hecke Curves on $Z_N$ and Conjecture 4

**Need:** a geometric interpretation of the condition “ $E \sim E'$ ” or “ $E \approx E'$ ”.

**Recall:** The modular curve  $X'_0(n) = X_0(n) \setminus \{\text{cusps}\}$  (coarsely) parametrizes the sets

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

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

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

induces morphisms

$$\tau_{n,k} : X'_0(n) \rightarrow Z_N \text{ and } \bar{\tau}_{n,k} : X_0(n) \rightarrow \bar{Z}_N.$$

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

**Remarks. 1)** The map  $\bar{\tau}_{n,k} : X_0(n) \rightarrow \bar{T}_{n,k}$  is finite and **birational**. Thus  $g(\bar{T}_{n,k}) = g(X_0(n))$  and hence

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

**2)** As the name suggests, the  $T_{n,k}$ 's are closely connected to the (irreducible) **Hecke correspondences**  $T_n = T(1, n)$  on  $X(N)$ :

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

**Conjecture 5:** If  $N \geq 23$  is **prime**, 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:

**Let**  $\bar{G}_N = G_N/\{\pm 1\} = \mathrm{SL}_2(\mathbb{Z}/N\mathbb{Z})/\{\pm 1\}$ .

**Proposition 1.** If  $N \geq 23$  is prime, then

(a)  $H < \bar{G}_N \Rightarrow g(H \backslash X(N)) \geq 2$ .

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

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

**However:**  $\exists$   $\infty$ 'ly many  $\Delta_{N,\varepsilon}$ -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 4** (Hermann) If  $N \equiv 7 \pmod{8}$  is prime and  $\varepsilon \equiv -1 \pmod{N}$ , then Conjecture 6 is true.

**Remark.** Conjecture 6 is true for  $N \leq 13$ .

## 5. The Néron-Severi Group of $Z_{N,\varepsilon}$

**Key Open Question:** If  $N = p \geq 23$ , is every curve  $C \subset \bar{Z}_{N,\varepsilon}$  of genus  $\leq 1$  a modular curve, i.e. of the form  $C = T_{n,k}$ ?

**Simpler Question:** Up to (algebraic) equivalence, are all the curves/divisors on  $\bar{Z}_{N,\varepsilon}$  modular?

**Notation:** Let  $NS^0(\bar{Z}_{N,\varepsilon}) = NS(\bar{Z}_{N,\varepsilon}) \otimes \mathbb{Q}$ , where  $NS(\bar{Z}_{N,\varepsilon})$  denotes the Néron-Severi group of  $\bar{Z}_{N,\varepsilon}$ , i.e.

$$NS(\bar{Z}_{N,\varepsilon}) = \text{Div}(\bar{Z}_{N,\varepsilon}) / (\text{algebraic equivalence}).$$

In addition, we write

$$\overline{NS}^0(Z_{N,\varepsilon}) = NS^0(Z_{N,\varepsilon}) / \langle cl(X_P), cl(X'_P) \rangle,$$

where  $X_P = \bar{\Phi}_{\mathbb{Q}}(X \times P)$  and  $X'_P = \bar{\Phi}_{\mathbb{Q}}(P \times X)$  for  $X = X(N)_{/\mathbb{Q}}$  and  $P \in X(\mathbb{Q})$ . Here, as above,  $\bar{\Phi}_{\mathbb{Q}}$  denotes the “quotient” map

$$\bar{\Phi}_{\mathbb{Q}} : X \times X \rightarrow \bar{Z}_{N,\varepsilon}.$$

**Recall:** The theory of correspondences shows that there is a close connection between the Neron-Severi group  $NS(X \times X)$  of the product surface and the endomorphism ring  $\text{End}_{\mathbb{Q}}(J_X)$  of its Jacobian  $J_X$ . Thus:

**Proposition 2.** We have a canonical identification

$$\overline{NS}^0(Z_{N,\varepsilon}) \simeq \text{End}_{G_{N,\varepsilon}}^0(J(N)),$$

where  $J(N) = J_{X(N)}$  and

$$\text{End}_{G_{N,\varepsilon}}^0(J(N)) = \{f \in \text{End}_{\mathbb{Q}}^0(J(N)) : gf = f\alpha_{\varepsilon}(g), \forall g \in G_N\}.$$

**Notation:** Let  $\mathbb{T}_{\varepsilon} \subset \text{End}_{\mathbb{Q}}^0(J(N))$  denote the  $\mathbb{Q}$ -vector space generated by the  $T_{n,k}$ 's with  $nk^2 \equiv \varepsilon \pmod{N}$ . Thus

$$\mathbb{T}_{\varepsilon} \subset \text{End}_{G_{N,\varepsilon}}^0(J(N)),$$

and

$$\sum_{\varepsilon} \mathbb{T}_{\varepsilon} = \langle T_n : (n, N) = 1 \rangle =: \mathbb{T}'.$$

**Theorem 5.** If  $N = p$  is prime, then

$$\overline{NS}^0(\bar{Z}_{p,\varepsilon}) \simeq \mathbb{T}_{\varepsilon}.$$

**Conclusion:** Thus, up to algebraic equivalence, all divisors in  $Z_{p,\varepsilon}$  are **modular**, i.e. they are  $\mathbb{Q}$ -linear combinations of the divisors  $\bar{T}_{n,k}$  with  $nk^2 \equiv \varepsilon (N)$ , together with the two curves  $X_P$  and  $X'_P$ .

**Theorem 6.** The rank of the Néron-Severi group (**Picard number**) is given by

$$\text{rk } NS(\bar{Z}_{p,\varepsilon}) = 2 + \frac{1}{24}(p-1)(p-5) + \frac{1}{2} \left( \frac{\varepsilon}{p} \right) h(p),$$

where

$$h(p) = \begin{cases} h(\mathbb{Q}(\sqrt{-p})) & \text{if } p \equiv 3(4) \\ 0 & \text{if } p \equiv 1(4) \end{cases}$$

**Remarks. 1)** The **proofs** of Theorems 5 and 6 depend on certain **structure theorems** for  $\text{End}^0(J(N))$ .

**2)** The analogous assertion of Theorem 5 for the Néron-Severi group of  $\bar{Z}_{N,\varepsilon} \otimes \mathbb{C}$  is **false** for two reasons:

1) There exist **modular curves** on  $\bar{Z}_{N,\varepsilon} \otimes \mathbb{C}$  which are not algebraically equivalent to linear combinations of the  $T_{n,k}$ 's;

2) The presence of **CM-elliptic curves** in  $J_{X(N)} \otimes \mathbb{C}$  gives rise to cycles which are **not modular**.

## 6. The Structure of $\text{End}_{\mathbb{Q}}^0(J(N))$

**Let**  $\Gamma$  be a congruence group with  $\Gamma_1(N) \leq \Gamma \leq \Gamma_0(N)$ ,

$X_{\Gamma} = \Gamma \backslash \mathfrak{H}^*$  be the associated modular curve,

$X = X_{\Gamma, \mathbb{Q}}$  its canonical model over  $\mathbb{Q}$ ,

$J = J_X$ , its Jacobian variety of dimension  $g_X$ ,

$\mathbb{E} = \text{End}_{\mathbb{Q}}^0(J) = \text{End}_{\mathbb{Q}}(J) \otimes \mathbb{Q}$ .

**Recall:**  $\mathbb{E}$  contains the (semi-simple) subalgebra

$$\mathbb{T}' = \langle T_n : n \geq 1, (n, N) = 1 \rangle \subset \mathbb{E}.$$

**Note:** If  $N = p$  is prime, then  $\mathbb{T}' = \mathbb{E}$  (Ribet), but in general these two algebras are different.

**Reason:** For each pair  $(M, d)$  with  $Md|N$ , there is a degeneracy morphism (Mazur)

$$B_{M,d} : X \rightarrow X_M,$$

where  $X_M$  is the corresponding curve of level  $M$ , and these give rise to new endomorphisms

$$D_{M,d} := B_{M,1}^* \circ (B_{M,d})_*, \quad {}^t D_{M,d} := B_{M,d}^* \circ (B_{M,1})_*$$

**Theorem 7.**  $\mathbb{E} = \langle \mathbb{T}', \{D_{M,d}, {}^t D_{M,d} : Md|N\} \rangle$ .

**Corollary.**  $Z(\mathbb{E}) = \mathbb{T}'$ .

**Remark.** The above result also applies to **other** modular curves such as  $X = X(N)$ . From this one obtains:

**Corollary.** If  $N = p$  is prime, then there exist  $\tau, \tau' \in \mathbb{Q}[G_N]$  such that

$$\text{End}_{\mathbb{Q}}^0(J(N)) = \langle \mathbb{T}', \tau, \tau' \rangle.$$

**Theorem 8.** If  $X = X(N)$ , then

$$\mathbb{T}' = \bigoplus_{\varepsilon} \mathbb{T}_{\varepsilon}.$$