Moduli Problems Attached to Isomorphisms of Elliptic Galois Representations

Ernst Kani
Queen's University at Kingston, Ontario, Canada

Alpbach Workshop
1 July 2018

Outline

1. Introduction

- Let:

E/K	be an elliptic curve over a number field K,
$N \geq 3$	a prime number,
$E[N]$	the group of N-torsion points of E
$\bar{\rho}_{E/K,N}$:	$G_K = \mathrm{Gal}(\overline{K}/K) \to \mathrm{Aut}(E[N]) \simeq \mathrm{GL}_2(\mathbb{Z}/N\mathbb{Z})$
	the associated Galois representation.

- It turns out that the study of isomorphisms of such Galois representations is closely related to many important problems and conjectures in Diophantine Geometry.
- Aim: To use various moduli spaces attached to such isomorphisms in order to illuminate these conjectures.

2. Some Conjectures

- The basic conjecture concerning isomorphisms of Galois representations is the following.
- Conjecture 1 (Frey, 1984). If E/K is an elliptic curve, then there is a constant $c_{E/K}$ such that $\forall$ prime numbers $N > c_{E/K}$ and all elliptic curves E'/K

$$(1) \qquad \bar{\rho}_{E/K,N} \simeq \bar{\rho}_{E'/K,N} \quad \Rightarrow \quad E \sim_K E'.$$

- Remark: Frey (1995) proved that Conjecture 1 for $K = \mathbb{Q}$ is equivalent to the asymptotic Fermat Conjecture.

2. Some Conjectures – 2

- Asymptotic Fermat Conjecture: For integers a, b, c with $abc \neq 0$ and a prime N let $C_{a,b,c;N}$ denote the twisted Fermat curve defined by

$$C_{a,b,c;N}: \quad aX^N - bY^N = cZ^N.$$

Then for every finite set S of primes we have that

$$\left| \bigcup_{N \geq 5} \bigcup_{a,b,c: sup(abc) \subset S} C_{a,b,c;N}(\mathbb{Q}) \right| < \infty.$$

Here $sup(n) = \{p|n : p \text{ is prime}\}$.

- Remark: It is easy to see that the ABC-Conjecture implies the Asymptotic Fermat Conjecture.

2. Some Conjectures – 3

- Frey's Conjecture can be generalized as follows.
- Conjecture 2 (Darmon, 1995). There is a constant c_K such that for all elliptic curves E/K and E'/K and all prime numbers $N > c_K$

$$(2) \qquad \bar{\rho}_{E/K,N} \simeq \bar{\rho}_{E'/K,N} \quad \Rightarrow \quad E \sim_K E'.$$

- Remarks: 1) Conjecture 2 is often called the Frey-Mazur Conjecture. Better: Darmon-Frey-Mazur Conjecture.
  2) There is some numerical evidence for the validity of this conjecture for $K = \mathbb{Q}$ (see below). Another is the following.
- Theorem 1: Conjecture 2 is true when restricted to pairs of elliptic curves with complex multiplication.

2. Some Conjectures – 4

- The following conjecture is also due to Darmon.
- Conjecture 3 (Darmon, 1995). There is an absolute constant $N_0 > 0$ such that for every $N > N_0$ and for every number field K the implication

$$\bar{\rho}_{E/K,N} \simeq \bar{\rho}_{E'/K,N} \quad \Rightarrow \quad E \sim_K E'$$

  holds for all except a finite number of pairs $(E/K, E'/K)$ of elliptic curves over K (up to simultaneous twists).
- Remark 1. The condition about simultaneous twists (which was missing in Darmon's formulation) is necessary because

$$\bar{\rho}_{E/K,N} \simeq \bar{\rho}_{E'/K,N} \quad \Rightarrow \bar{\rho}_{E_\chi/K,N} \simeq \bar{\rho}_{(E')_\chi/K,N}.$$

  for any (quadratic) twist $\chi : G_K \to \{\pm 1\}$.

2. Some Conjectures – 5

- Remark 2. Darmon's Conjecture 3 does not directly imply Frey's Conjecture, and hence it also does not imply Conjecture 2. Similarly, Conjecture 2 does not imply Conjecture 3.
- Remark 3. In 1995 I refined Darmon's Conjecture 3 as follows.
- Conjecture 3*. Conjecture 3 holds with $N_0 = 23$.

3. Mazur's Question

- The above conjectures were perhaps motivated in part by the following question posed by Mazur in 1978.
- Question (Mazur, 1978). Are there two non-isogenous elliptic curves $E/\mathbb{Q}$ and $E'/\mathbb{Q}$ and a prime $N \geq 7$ such that $\bar{\rho}_{E/\mathbb{Q},N}$ and $\bar{\rho}_{E'/\mathbb{Q},N}$ are symplectically isomorphic?
- Answer: Yes! (Kraus/Oesterlé, 1992). In fact, $\exists$ infinitely many such pairs for $N = 7$ (Halberstadt/Kraus, 1997). Moreover: the same is true for $N = 11$ (K./Rizzo, 1999).
- But: For $N \geq 13$, only finitely many such pairs are known via computer calculations. Largest for $N = 17$ (Billerey, 2016).
- Note: This gives some computational evidence for the validity of Conjecture 2.

3. Mazur's Question – 2

- The above results naturally lead to the following questions:
  - Why did Mazur impose the bound $N \geq 7$ in his question?
  - Why are there infinitely many pairs $(E/\mathbb{Q}, E'/\mathbb{Q})$ which solve Mazur's Question for $N = 7, 11$, but only finitely many (are known to) exist for $N > 11$?
- The answer to both questions: Diophantine properties of certain Moduli spaces!

4. The Modular Curves $X_{E,N}$ and $X_{E,N,\varepsilon}$

- In connection with Frey's Conjecture and Mazur's Question, it is useful to fix the elliptic curve E/K and the integer N and to consider for any extension field L/K the sets

$$\mathcal{X}_{E/K,N}(L) := \{(E'/L, \psi) | \psi : \bar{\rho}_{E/L,N} \xrightarrow{\sim} \bar{\rho}_{E'/L,N}\}/\simeq .$$

- By viewing G_L-isomorphisms of these Galois representations as isomorphisms of the associated L-group schemes $E[N]$ and $E'[N]$, it is easy to see that this extends to a functor

$$\mathcal{X}_{E/K,N} : (\mathrm{Sch}/K) \to (\mathrm{Sets})$$

from the category (Sch/K) of K-schemes to the category (Sets) of sets.

4. The Modular Curves $X_{E,N}$ and $X_{E,N,\varepsilon}$ – 2

- Proposition 1. If $N \geq 3$, then $\mathcal{X}_{E/K,N}$ is represented by a smooth affine curve $X_{E/K,N}/K$. Moreover,

$$X_{E/K,N} = \coprod_{\varepsilon \in (\mathbb{Z}/N\mathbb{Z})^\times} X_{E/K,N,\varepsilon}$$

- Remark. Each component $X_{E/K,N,\varepsilon}/K$ represents the subfunctor $\mathcal{X}_{E/K,N,\varepsilon}$ of $\mathcal{X}_{E/K,N}$ which is defined by

$$\mathcal{X}_{E/K,N,\varepsilon}(L) = \{(E', \psi) \in \mathcal{X}_{E/K,N}(L) : \det(\psi) = \varepsilon\}.$$

Here $\varepsilon = \det(\psi)$ is the unique $\varepsilon \in (\mathbb{Z}/N\mathbb{Z})^\times$ such that

$$e_N^{E'}(\psi(x), \psi(y)) = e_N^E(x, y)^{\det(\psi)}, \quad \forall x, y \in E[N](\bar{K}),$$

where $e_N^E(\cdot, \cdot)$ denotes the (Weil) e_N-pairing on $E[N]$.

4. The Modular Curves $X_{E,N}$ and $X_{E,N,\varepsilon}$ – 3

- Addendum. Each component $X_{E/K,N,\varepsilon}$ is a twist of the (affine) modular curve $X(N) = \Gamma(N)\backslash\mathfrak{H}$ and hence is geometrically irreducible. Thus, the genus of its compactification $\bar{X}_{E/K,N}$ is ≥ 3 when $N \geq 7$ and is ≤ 1 when $N < 7$.
- Consequence: The fact that $X_{E/K,N}$ represents the functor $\mathcal{X}_{E/K,N}$ implies that we have for each extension field L/K a bijection

$$\mathcal{X}_{E/K,N}(L) \overset{\sim}{\to} X_{E/K,N}(L)$$

  when $N \geq 3$. Thus, by the Theorem of Faltings we know that for each $N \geq 7$ the set $\mathcal{X}_{E/K,N}(K)$ is finite! On the other hand, if $N < 7$, then we expect $\mathcal{X}_{E/K,N}(K)$ to be infinite.
- Similar assertions hold for $\mathcal{X}_{E/K,N,\varepsilon}$ and $X_{E/K,N,\varepsilon}$.

4. The Modular Curves $X_{E,N}$ and $X_{E,N,\varepsilon}$ – 4

- Note that Mazur's Question concerns the sets

$$\mathcal{X}_{E/\mathbb{Q},N,1}(\mathbb{Q}) \xrightarrow{\sim} X_{E/\mathbb{Q},N,1}(\mathbb{Q}),$$

  for all elliptic curves $E/\mathbb{Q}$ and all $N \geq 7$. Thus, the above Consequence explains in part why Mazur focused on the case $N > 7$.

- Remark. Proposition 1 follows easily from the general results presented in the book *Arithmetic Moduli of Elliptic Curves* by Katz and Mazur (1985).

5. The Modular Surfaces Z_N and $Z_{N,\varepsilon}$

- In view of Darmon's Conjectures and Mazur's Question, it is natural to consider for a fixed N and field K the set

$$\mathcal{Z}_N(K) := \{(E, E', \psi)\}/\simeq$$

of K-isomorphism classes of triples (E, E', ψ) consisting of two elliptic curves E/K and E'/K and an isomorphism $\psi : E[N] \xrightarrow{\sim} E'[N]$ of K-group schemes.
Again, this extends to a functor $\mathcal{Z}_N : (\mathrm{Sch}/\mathbb{Q}) \to (\mathrm{Sets})$.
- Moreover, for each $\varepsilon \in (\mathbb{Z}/N\mathbb{Z})^\times$ put

$$\mathcal{Z}_{N,\varepsilon}(K) := \{(E, E', \psi) : \det(\psi) = \varepsilon\}/\simeq,$$

and extend this to a functor $\mathcal{Z}_{N,\varepsilon} : (\mathrm{Sch}/\mathbb{Q}) \to (\mathrm{Sets})$.

5. The Modular Surfaces Z_N and $Z_{N,\varepsilon}$ - 2

- Proposition 2. The functors $\mathcal{Z}_N$ and $\mathcal{Z}_{N,\varepsilon}$ are coarsely represented by affine normal surfaces $Z_N/\mathbb{Q}$ and $Z_{N,\varepsilon}/\mathbb{Q}$, respectively, and we have

$$Z_N = \coprod_{\varepsilon \in (Z/N\mathbb{Z})^\times} Z_{N,\varepsilon}.$$

Each $Z_{N,\varepsilon} \otimes \mathbb{C}$ is a finite quotient of the product surface $X(N) \times X(N)$ and hence $Z_{N,\varepsilon}$ is geometrically irreducible.

- Remark. The fact that Z_N coarsely represents $\mathcal{Z}_N$ implies that we have maps

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

which are compatible with field extensions and which are bijections when K is algebraically closed.

5. The Modular Surfaces Z_N and $Z_{N,\varepsilon}$ - 3

- Proposition 3 (K./Rizzo, 1999). If K is a number field, then $\mu_{N,K} : \mathcal{Z}_N(K) \to Z_N(K)$ is surjective. On the other hand, $\mu_{N,K}$ is never injective but it is injective modulo simultaneous twists.
- The geometric nature of the surfaces $Z_{N,\varepsilon}$ is fairly well understood:
- Theorem 2 (Hermann, 1991; K./Schanz, 1997). Let $\bar{Z}_{N,\varepsilon}$ be the compactification of the affine surface $\bar{Z}_{N,\varepsilon}$ and let $\tilde{Z}_{N,\varepsilon}$ denote its desingularization. Then $\tilde{Z}_{N,\varepsilon}$ is of general type if and only if $N \geq 13$. Furthermore, $\tilde{Z}_{7,1}$ is a rational surface and $\tilde{Z}_{11,1}$ is an elliptic surface.
- Remark. Since surfaces of general type are expected to have fewer K-rational points than other surfaces, this gives a partial answer to the question of why there were many isomorphisms of Galois representations for $N = 7, 11$ and few for $N \geq 13$.

6. Modular Correspondences

- The surfaces Z_N and $Z_{N,\varepsilon}$ give us a geometric framework for studying isomorphisms of elliptic Galois representations. However, in order to understand Darmon's Conjectures 2 and 3 in this context, we also need to have a geometric description of when two elliptic curves are isogenous. For this, recall:
- Fact: Let $\mathcal{X}_0(m) : (\mathrm{Sch}/\mathbb{Q}) \to (\mathrm{Sets})$ denote the functor of cyclic m-isogenies, i.e.,

$$\mathcal{X}_0(m)(K) = \{(E, E', f)\}/\simeq$$

where $f : E \to E'$ is a cyclic K-isogeny of degree m. Then the modular curve $X_0(m)/\mathbb{Q}$ is a coarse moduli space for the functor $\mathcal{X}_0(m)$.

6. Modular Correspondences - 2

- Observation. If $\gcd(km, N) = 1$, then the rule $(E, E', f) \mapsto (E, E', kf_{|E[N]})$ defines a morphism of functors

$$\tau_{N,m,k} : \mathcal{X}_0(m) \ \to \ \mathcal{Z}_N$$

  and hence a morphism of $\mathbb{Q}$-schemes $\tau_{N,m,k} : X_0(m) \ \to \ Z_N$ which is birational onto its image $T_{N,m,k} := \tau_{N,m,k}(X_0(m))$.
- Remarks. 1) $T_{N,m,k} \subset Z_{N,mk^2} \subset Z_N$.
  2) Recall that the product surface $X(N) \times X(N)$ comes equipped a with distinguished set of curves called modular correspondences. Via the quotient map

$$\Phi_{N,\varepsilon} : X(N) \times X(N) \to Z_{N,\varepsilon} \otimes \mathbb{C},$$

  these give curves on $Z_{N,\varepsilon} \otimes \mathbb{C} \subset Z_N \otimes \mathbb{C}$ which we'll call modular correspondences on Z_N. It turns out that the curves $T_{N,m,k}$ are such modular correspondences on Z_N.

6. Modular Correspondences - 3

- Observation. The genus of the curve $X_0(m)$ has the following property:

$$g(X_0(m)) \leq 1 \;\Leftrightarrow\; m \leq 27 \text{ and } m \neq 22, 23, 26.$$

  Thus, if K is sufficiently large, then each of these curves has infinitely K-rational points and so the same is true for the $T_{N,m,k}$'s.
- Thus: by Proposition 3 these lead to infinitely many pairs of isomorphic Galois representations over K. However, these all belong to pairs of isogenous elliptic curves.
- Can we expect many other pairs?

7. Further Conjectures

- Recall: The key ingredient for understanding the arithmetic of the 1-dimensional moduli problem $X_{E/K,N}$ was Mordell's Conjecture ($=$ Theorem of Faltings). The analogue of this conjecture/theorem for higher dimensions is Lang's Conjecture. For surfaces, this can be stated as follows.
- Conjecture 4 (Lang). If Z/K is a surface of general type, then:

  (a) The surface $Z \otimes \bar{\mathbb{Q}}$ contains only finitely many curves C of genus $g(C) \leq 1$, so their union Z_{exc} is a closed subset of Z.

  (b) For every number field $L \supset K$, the set $Z(L) \setminus Z_{exc}(L)$ is finite.
- Question. What is the exceptional set $(Z_N)_{exc}$ of Z_N?

7. Further Conjectures - 2

- Proposition 4. If T is any modular correspondence on Z_N, then $g(T) \leq 1 \Leftrightarrow T = T_{N,m,k}$, for some $m \leq 27$ with $m \neq 22, 23, 26$.
- This and other considerations led me in 1995 to make the following conjecture.
- Conjecture 5 (K., 1995). If $N \geq 23$ is prime, then every curve $C \subset Z_N$ of genus 0 or 1 is modular; i.e., $C = T_{N,m,k}$ with $m \leq 27$ and $m \neq 22, 23, 26$.
- Proposition 5. If Lang's Conjecture holds for the Z_N's and if Conjecture 5 holds, then the refined Darmon's Conjecture 3* is true.

7. Further Conjectures - 3

- Recently Bakker and Tsimerman proved the following amazing result.
- Theorem (Bakker/Tsimerman, 2013) There exists an N_0 such that if $N > N_0$ is prime, then $(Z_N)_{exc}$ consists only of modular correspondences.
- Corollary. Lang's Conjecture implies Darmon's Conjecture 3.
- Unfortunately: it is unknown how large the constant N_0 in the BT-Theorem is.

8. The Basic Construction

- By construction, the surface $Z_{N,\varepsilon}$ is the coarse moduli space of the functor $\mathcal{Z}_{N,\varepsilon}$ of isomorphisms of elliptic Galois representations of determinant $\varepsilon \in (\mathbb{Z}/N\mathbb{Z})^\times$.
  But in the case that $\varepsilon \equiv -1 \pmod N$, the surface $Z_{N,-1}$ also has another interpretation in terms of Hurwitz spaces, as we shall see. The basis for this is:
- The basic construction (Frey/K., 1991). Let $(E, E', \psi) \in \mathcal{Z}_{N,-1}(K)$, so $\psi : E[N] \xrightarrow{\sim} E'[N]$ is an anti-isometry. Put

  $$A_\psi \;=\; (E \times E')/\mathrm{Graph}(\psi).$$

  Then A_ψ carries a unique (K-rational) principal polarization

  $$\lambda_\psi : A_\psi \;\xrightarrow{\sim}\; \hat{A}_\psi$$

  such that its pull-back to $E \times E'$ is a multiple of the product polarization on $E \times E'$.

8. The Basic Construction - 2

- Notation. Let $\mathcal{A}_2 : (\mathrm{Sch}/\mathbb{Q}) \to (\mathrm{Sets})$ denote the moduli functor of principally polarized abelian surfaces, i.e.,

$$\mathcal{A}(K) = \{(A, \lambda)\}/\simeq,$$

  where A/K is an abelian surface and $\lambda : A \xrightarrow{\sim} \hat{A}$ is a K-rational principal polarization.

- Proposition 5. The basic construction defines a morphism of functors

$$\beta_N : \mathcal{Z}_{N,-1} \to \mathcal{A}_2,$$

  and the induced morphism $\beta_N : Z_{N,-1} \to A_2$ on the coarse moduli spaces is a finite morphism.

- Remark. The image of β_N is the Humbert surface Hum_{N^2} with Humbert invariant N^2.

8. The Basic Construction - 3

- In the case of Jacobians, the basic construction also yields curve covers.
- Proposition 6. Let $(E, E', \psi) \in \mathcal{Z}_{N,-1}(K)$. If $(A_\psi, \lambda_\psi) \simeq (J_C, \lambda_C)$ is the Jacobian of a curve C/K, then there exists a K-cover $f : C \to E$ of degree N.
  Moreover, f is *minimal* (i.e., f does not factor over an isogeny of E of degree > 1), and the equivalence class of f is uniquely determined by the condition that $f^* : E \simeq J_E \to J_C$ equals $\pi \circ i_E$, where $\pi : E \times E' \to A_\psi \simeq J_C$ is the quotient map and $i_E : E \hookrightarrow E \times E'$ the canonical inclusion.
- Definition. Two curve covers $f_i : X_i \to Y$ are *equivalent* if there exists an isomorphism $\varphi : X_1 \xrightarrow{\sim} X_2$ and an automorphism $\alpha \in \mathrm{Aut}(Y)$ such that $\alpha \circ f_1 = f_2 \circ \varphi$.
  If this holds with $\alpha = 1_Y$, then the covers are *isomorphic*.

9. Hurwitz Spaces

- Recall: Let $Y/\mathbb{C}$ be a curve. Hurwitz showed in 1898 that the set of isomorphism classes of curve covers $f : X \to Y$ of bounded degree and genus can be identified with the points of an analytic space (now called a Hurwitz space.)
  Here we construct a (restricted) Hurwitz space of genus 2 covers of an elliptic curve.
- Definition. Let E/K be an elliptic curve and C/K a curve of genus 2. A cover $f : C \to E$ of degree N is said to be *normalized* if

  (i) f is minimal;

  (ii) $[-1]_E \circ f = f \circ \omega_C$, where ω_C is the hyperelliptic involution on C;

  (iii) $\deg(f^*(0_E) \cap W_C) = 3\mathrm{rem}(N, 2)$, where $W_C = \mathrm{Fix}(\omega_C)$ is the divisor of Weierstraß points.
- Lemma. If $f : C \to E$ is a minimal K-cover, then there exists a unique $x \in E(K)$ such that $T_x \circ f$ is normalized.

9. Hurwitz Spaces - 2

- Fix an elliptic curve E/K and an integer N. If L/K is an extension field, put

  $$\mathcal{H}_{E/K,N}(L) := \{C \xrightarrow{f} E \text{ is a normalized } L\text{-cover of degree } N\}/\simeq$$

  By using the basic construction one obtains:

- Theorem 2 (K., 2003). The assignment $L \mapsto \mathcal{H}_{E/K,N}(L)$ extends to a functor $\mathcal{H}_{E/K,N} : (\mathrm{Sch}/K) \to (\mathrm{Sets})$.
  If $N \geq 3$, then this functor is represented by an open subset $H_{E/K,N}$ of the curve $X_{E/K,N,-1}$.
  In particular, $H_{E/K,N} \otimes \mathbb{C}$ is an open subset of $X(N)$, and $H_{E/K,N}$ is a smooth, affine curve which is geometrically irreducible.

- Corollary. If E/K is an elliptic curve a number field K, then there are only finitely many normalized K-covers $f : C \to E$ of fixed degree $N \geq 7$.

9. Hurwitz Spaces - 3

- In the above Hurwitz space we had fixed the base elliptic curve E/K. We now consider the case that we allow E/K to vary. In this case we have to consider equivalence classes of covers: $(f_1 : C_1 \to E_1) \sim (f_2 : C_2 \to E_2) \Leftrightarrow \exists \varphi : C_1 \xrightarrow{\sim} C_2, \alpha : E_1 \xrightarrow{\sim} E_2 : \alpha \circ f_1 = f_2 \circ \varphi.$
  If L is any extension field of $\mathbb{Q}$, put

  $$\mathcal{H}_N(L) := \{f : C \to E \text{ is a normalized } L\text{-cover of degree } N\}/\sim$$

  Similar to before, the assignment $L \mapsto \mathcal{H}_N(L)$ extends to a functor $\mathcal{H}_N : (\mathrm{Sch}/\mathbb{Q}) \to (\mathrm{Sets})$.
- Theorem 3 (Frey/K., 2009). If $N \geq 3$, then $\mathcal{H}_N$ is coarsely represented by an open subset H_N of $Z_{N,-1}$.

9. Hurwitz Spaces - 4

- Remark. The "boundary" $\partial H_N := Z_{N,-1} \setminus H_N$ can be described explictly since it is always a union of modular correspondences on $Z_{N,-1}$.
  In the case that N is prime, the components of ∂H_N are the curves $T_{N,m,k}$ with $m = \frac{s(N-s)}{t^2}$, where $1 \leq s \leq \frac{N-1}{2}$ and $t^2 | s(N-s)$, and $ks \equiv \pm 1 \pmod{N}$.

10. The Discriminant

- In the classical theory of Hurwitz spaces, which classifies covers up to isomorphism, the discriminant divisor $\mathrm{disc}(f)$ of the cover f plays an important role. In our situation we have:
- Proposition 7. Let E/K be an elliptic curve and let $\pi_E : E \to E/\langle[-1]_E\rangle \simeq \mathbb{P}^1_K$ be the (Weierstraß) quotient map. If $N \geq 3$ is an integer, then there exists a morphism

$$\delta_{E/K,N} : H_{E/K,N} \ \to \ \mathbb{P}^1_K$$

such that $\mathrm{disc}(f_x) = \pi_E^*(\delta_{E/K,N}(x))$, for all $x \in H_{E/K,N}(K)$, where $f_x : C_x \to E$ is the cover corresponding to x. In particular, if $\bar{P} \in \mathbb{P}^1_K(K)$, then

$$\delta^{-1}_{E/K,N}(\bar{P})(K) = \{x \in H_{E/K,N}(K) : \mathrm{disc}(f_x) = \pi_E^*(P)\}.$$

- It is much more difficult is to determine the degree of $\delta_{E/K,N}$.

10. The Discriminant - 2

- Theorem 3 (K., 2006). If $N \geq 3$, then $\delta_{E/K,N}$ is unramified outside of $\pi_E(E[2])$ and its degree is

$$\deg(\delta_{E/K,N}) = \frac{1}{12}(N-1)sl(N),$$

where

$$sl(N) = |\,\mathrm{SL}_2(\mathbb{Z}/N\mathbb{Z})| = N\phi(N)\psi(N) = N^3 \prod_{P|N}(1 - \frac{1}{p^2}).$$

- Remark. This is proved (in K. 2006) by compactifying the universal cover

$$f_u : \mathcal{C} \to E \times H_{E,K}$$

and interpreting $\deg(\delta_{E/k})$ as an intersection number on the compactified surface $\bar{\mathcal{C}}$. The key ingredients for computing this intersection number are (i) a detailed study of the degenerate fibres of the (semi-stable) fibration $\bar{p} : \bar{\mathcal{C}} \to \bar{X}(N)$ and (ii) certain identities due to Noether and Mumford between the Faltings height $h_{\bar{\mathcal{C}}/\bar{X}(N)}$ and other invariants of the fibration (called δ_0 and δ_1).

10. The Discriminant - 3

- Corollary. If $D \in \mathrm{Div}(E)$ is a effective divisor of degree 2, and if $N \geq 3$ is an integer, then the number of minimal genus 2 covers of degree N of $E/\bar{K}$ with discriminant D is

$$|\mathrm{Cov}^{(min)}_{E/\bar{K},N,D}| = \tfrac{1}{3\mu_D}(N-1) - \frac{\mu_D - 1}{6N} sl(N),$$

where $\mu_D = 1$ if D is reduced and $\mu_D = 2$ otherwise.

- Remark. It is also possible to deduce from this the weighted number $\bar{c}_{E,D} = \sum_{f \in Cov_{E,N,D}} 1/|\mathrm{Aut}(f)|$ of genus 2 covers of $E/\bar{K}$ of degree N with discriminant D:

$$\bar{c}_{E,D} = \tfrac{N}{3\mu_D}(\sigma_3(N) - N\sigma_1(N)) - \tfrac{\mu_D - 1}{24}(7\sigma_3(N) - (6N+1)\sigma_1(N))),$$

where $\sigma_k(n) = \sum_{d|n} d^k$. This formula (for D reduced) was derived by by Dijkgraaf (1995) by using mirror symmetry (and group theory).

11. The Discriminant Stratification of H_N

- While the discriminant $\mathrm{disc}(f) \in \mathrm{Div}(E)$ is clearly an invariant of the isomorphism class of the cover f, this is no longer the case when we pass to the equivalence class of f. Thus, we cannot naturally "extend" the discriminant morphism $\delta_{E/K,N}$ on $H_{E/K,N}$ to a morphism on H_N.
- However: certain properties of $\mathrm{disc}(f)$ (for normalized covers) are preserved under equivalence:
  - $\mathrm{disc}(f)$ is reduced;
  - $\mathrm{disc}(f) = 2O_E$;
  - $\mathrm{disc}(f) = 2P$, where $P \in E[2] \setminus \{0_E\}$.

  These, therefore, give rise to subsets $H_N^{(red)}$, $H_N^{(0)}$ and $H_N^{(2)}$, respectively, and H_N is the disjoint union of these. Thus we have the stratification

$$H_N = H_N^{(red)} \coprod H_N^{(0)} \coprod H_N^{(2)}.$$

- Proposition 8. H^{red} is an open affine subset of H_N, and $H_N^{(0)}$ and $H_N^{(2)}$ are (reducible) curves.

The Discriminant Stratification of H_N - 2

- Remark. Certain irreducible components of $H_N^{(0)}$ and of $H_N^{(2)}$ have been studied extensively from the point of view of Teichmüller curves which occur in the dynamics of billards (in polygons) and are described by square-tiled surfaces (and their deformations).
- For example: in the notation of McMullen (2005), we have the following (irreducible) Teichmüller curves $W^*_{N^2}$:
  - If $N \geq 4$ is even: $W_{N^2} \subset H_N^{(2)}$;
  - If $N \geq 5$ is odd: $W^0_{N^2} \subset H_N^{(2)}$ and $W^1_{N^2} \subset H_N^{(0)}$.

The Discriminant Stratification of H_N - 3

- Remark. It follows from the work of Hubert/Lelièvre (2006) that (for $N \geq 5$ prime) none of these Teichmüller curves can be modular correspondences because they are quotients of $\mathfrak{H}$ by non-congruence subgroups of $\mathrm{SL}_2(\mathbb{Z})$.
  Moreover, it follows from Lelièvre/Royer (2006) and the above Corollary of Theorem 3 that the curves $H^{(0)}$ and $H^{(2)}$ cannot be Teichmüller curves; i.e., there is at least one non-Teichmüller component.
- Proposition 9*. If $N \geq 11$, then every Teichmüller curve on $Z_{N,-1}$ has genus ≥ 3.
- Remark. This can be seen as further evidence for my Conjecture 5.