Mazur's question on mod 11 representations of elliptic curves *

E.J. Kani and O.G. Rizzo

1 Introduction

In 1978, Barry Mazur [14] asked the following question:

Question 1. *Do there exist two elliptic curves $E_1/\mathbb{Q}$, $E_2/\mathbb{Q}$ which are not isogenous $/\mathbb{Q}$ such that their associated Galois representations*

$$\overline{\rho}_{E_i,N} : \mathrm{Gal}(\bar{\mathbb{Q}}/\mathbb{Q}) \to \mathrm{Aut}(E_i[N])$$

are (symplectically) isomorphic for some $N \geq 7$?

In 1992 Kraus and Oesterlé [12] found the first such examples for $N = 7$, and recently Halberstadt and Kraus [5] exhibited explicit infinite families with this property (for $N = 7$).

For larger N, Mazur found examples for $N = 11$ and $N = 13$. In addition, Frey and his group have found many examples by computer [4].

The purpose of this paper is to prove the following result:

Theorem 2. *There exist infinitely many one-parameter families of isomorphism classes of pairs of non-isogenous elliptic curves defined over $\mathbb{Q}$ with symplectically isomorphic 11-structure.*

The main idea of the proof of this Theorem is to study the geometry (and arithmetic) of the *modular diagonal quotient surfaces* $Z_{N,1}$ (as introduced in [9]) in the special case $N = 11$. Now the algebraic surface $Z = Z_{N,1}$ has a natural model as a variety over $\mathbb{Q}$ (cf. §3), and an open subvariety of this turns out to be the coarse moduli space of the moduli functor $\mathcal{Z}_{N,1}$ which classifies isomorphism classes of triplets (E_1, E_2, ψ), where $\psi : E_1[N] \to E_2[N]$ is a $\mathrm{Gal}(\bar{\mathbb{Q}}/\mathbb{Q})$-isomorphism which preserves the Weil pairings. Thus, via this modular interpretation (cf. §4), the above Theorem is essentially a consequence of the following result (cf. Theorem 19):

*This research was partially supported by a grant from the Natural Sciences and Engineering Research Council of Canada (NSERC).

Theorem 3. *Let $\bar{Z}_{\mathbb{Q}}$ denote the minimal model of $Z_{11,1}/\mathbb{Q}$. Then the canonical map defines an elliptic fibration $f_{\text{can}} : \bar{Z}_{\mathbb{Q}} \to \mathbb{P}^1_{\mathbb{Q}}$ which has an infinite number of sections.*

Indeed, by using the result of Mazur [14] (as supplemented by Kenku [11]) on rational isogenies, one easily concludes that all except finitely many of these sections $S_i/\mathbb{Q} \simeq \mathbb{P}^1_{\mathbb{Q}}$ give rise to infinitely many pairs of non-isogenous elliptic curves.

It is interesting to observe that, although the above proof is constructive "in principle," it does not allow us to write down even a single pair explicitly. The reason for this is that, while the sections are constructed as the multiples of an explicit point Q of infinite order on the associated elliptic curve $\mathcal{E}/\mathbb{Q}(t)$, the point Q itself *does not* have a modular interpretation (since it lies in the *cuspidal part*), and its multiples nQ cannot be interpreted explicitly until the elliptic curve $\mathcal{E}$ can be determined.

2 Geometric results

2.1 The geometry of $\tilde{Z}$

We recall some of the terminology and results of [9]. Let N be a positive integer and let $X(N) = \Gamma(N)\backslash\mathbb{H}^*$ be the modular curve of level N, on which $G_N = \mathrm{SL}_2(\mathbb{Z}/N\mathbb{Z})/\pm\mathbf{1}$ acts naturally. We denote the quotient map by $\pi : X(N) \to X(1) = G_N\backslash X(N)$. Furthermore, let $Z = Z_{N,1} = \Delta\backslash(X(N) \times X(N))$ denote the (singular) *modular diagonal quotient surface*; here $\Delta = \big\{(g,g) : g \in G_N\big\}$ denotes the diagonal subgroup. Then (as in [9]) the inclusion of the subgroups $\{1\} \le \Delta \le G_N \times G_N$ induces natural maps

$$X(N) \times X(N) \xrightarrow{\Phi} Z \xrightarrow{\Psi} X(1) \times X(1)$$

such that $\Psi \circ \Phi = \pi \times \pi : X(N) \times X(N) \to X(1) \times X(1)$ is the natural projection.

Consider the points i, $\exp(2\pi i/3)$ and ∞ of $\mathbb{H}^*$, and let $\bar{P}_k$ (for $k = 0, 1, \infty$) be their respective images in $X(1)$.

For the remainder of the section, let $N = 11$. By Theorem 2.1 of [9], we have:

Proposition 4. *If $Z = Z_{11,1}$, then*

1. *The set of singularities of Z decomposes into $\Sigma_0 \cup \Sigma_1 \cup \Sigma_\infty$, where $\Sigma_k \subset \Psi^{-1}(\bar{P}_k, \bar{P}_k)$ for $k = 0, 1, \infty$. All singularities are cyclic quotient singularities.*

2. *Σ_0 consists of 6 singularities of type $(2, 1)$.*

3. *Σ_1 consists of 2 singularities of type $(3, 1)$ and of 2 singularities of type $(3, 2)$.*

4. *$\Sigma_\infty = \{z_1, \ldots, z_5\}$, where z_i is a singularity of type $(11, q_i)$ with $q_i \equiv \left(\frac{i}{11}\right) i \mod 11$ and $1 \leq q_i \leq 11$.*

Let $\sigma : \tilde{Z} \to Z$ be the minimal desingularization of Z. If C is a curve on Z, we will denote its proper transform on $\tilde{Z}$ by $\tilde{C}$.

Recall that the minimal desingularization of a cyclic quotient singularity of type (n, q) is a $(-n_1, \ldots, -n_r)$-chain, where r and $n_1, \ldots, n_r$ are determined by the continued fraction expansion of n/q (cf. [1, § III.2]). Here, by a $(-n_1, \ldots, -n_r)$-chain we mean an open chain $C = C_1 + \cdots + C_r$ of smooth rational curves C_i such that $C_i^2 = -n_i$, for $i = 1, \ldots, r$.

Let $\Psi_i = pr_i \circ \Psi : Z \to X(1) \simeq \mathbb{P}^1$, where $i = 1, 2$ and pr_i is the projection on the i-th factor of $X(1) \times X(1)$. Let $\tilde{\Psi}_i = \Psi_i \circ \sigma$.

Proposition 2.5 of [9] implies that:

Proposition 5. *For $k = 0, 1, \infty$, let E_k denote the reduced divisor on $\tilde{Z}$ whose support is $\sigma^{-1}(\Sigma_k)$, and let $E_{\infty,i}$ be the reduced divisor on $\tilde{Z}$ whose support is $\sigma^{-1}(z_i)$. Then*

1. *E_0 consists of six (disjoint) (-2)-curves;*

2. *E_1 consists of two (-2)-curves and of two $(-2, -2)$-chains;*

3. *$E_\infty = E_{\infty,1} + \cdots + E_{\infty,5}$, where*

   $E_{\infty,1}$ is a (-11)-curve,
   $E_{\infty,2}$ is a $(-4, -3)$-chain,
   $E_{\infty,3}$ is a $(-3, -2, -2, -2, -2)$-chain,
   $E_{\infty,4}$ is a $(-2, -2, -2, -2, -3)$-chain,
   $E_{\infty,5}$ is a $(-3, -4)$-chain.

Furthermore, if $\tilde{C}_{k,i}$ denotes the proper transform of $\Psi_i^*(\bar{P}_k)$ in $\tilde{Z}$, then each chain in E_k joins $\tilde{C}_{k,1}$ to $\tilde{C}_{k,2}$, where $k = 0, 1, \infty$.

2.2 The elliptic fibration

Notation. Let $n \not\equiv 0 \bmod 11$ be a positive integer which is a square modulo 11. Fix a $k \in \mathbb{F}_{11}^{\times}$ such that $k^2 n \equiv 1 \mod 11$ and let $\tau_k = \left(\begin{smallmatrix} 1/k & 0 \\ 0 & k \end{smallmatrix}\right) \in G_{11}$. Let $T_n = \Phi\left((\tau_k^{-1} \times \mathbf{1})T'(1,n)\right)$, where $T'(1,n)$ is the Hecke correspondence of $X(11) \times X(11)$ as defined in §3.3 of [16]. We call such a curve on Z a *Hecke curve.*

Remark 6. T_n is the curve $T_{n,k}$ of [9] or one of the curves $F_n^{(i)}$ of [6].

Proposition 7. *a) The (lifted) Hecke curves $\tilde{T}_1$, $\tilde{T}_3$ and $\tilde{T}_4$ are exceptional (-1)-curves on $\tilde{Z}$. Moreover, $\tilde{T}_1$ meets precisely three components of $E_0 + E_1 + E_\infty$: a (-2)-curve $\Gamma_0 \leq E_0$, a (-3)-curve $\Gamma_1 \leq E_1$ and $E_{\infty,1}$. In addition, $\tilde{T}_1$ meets each of these components transversely.*

b) Let $\bar{Z}$ be the surface obtained by blowing down $\tilde{T}_1$, Γ_0, Γ_1; $\tilde{T}_3$; $\tilde{T}_4$. Then $\bar{Z}$ is minimal.

Proof. The assertions of part (a) follow from Claims 3 and 4 of [9] and Remark 4.9 of [8]—but see also [6]. Part (b) is Claim 8 of [9]. □

Notation. If C (or $\tilde{C}$) is a curve on $\tilde{Z}$, denote its image in $\bar{Z}$ by $\bar{C}$.

Proposition 8. *Let S_0 (resp. S_1) be the (-4)-component of $E_{\infty,2}$ (resp. $E_{\infty,5}$). Then their images $\bar{S}_0$ and $\bar{S}_1$ on $\bar{Z}$ satisfy $S_0^2 = S_1^2 = -3$ and $S_0 \cdot S_1 = 1$.*

Proof. See the proof of Claim 4 of [9]. □

Theorem 9. *Let f_{can} be the canonical map of $\bar{Z}$. Then*

1. *$f_{\mathrm{can}} : \bar{Z} \to \mathbb{P}^1$ is an elliptic fibration with no multiple fibres.*
2. *$\bar{S}_0$ and $\bar{S}_1$ are sections of f_{can}.*
3. *Let E be the elliptic curve over $\mathbb{C}(t)$ corresponding to $(\bar{Z}, \bar{S}_0)$ and let Q be the point of E corresponding to $\bar{S}_1$. Then Q has infinite order on E.*

Proof. We know from (the proof of) [9], Proposition 2.14, that $\bar{Z}$ is a minimal smooth surface with geometric genus $p_g(\bar{Z}) = 2$, Euler–Poincaré characteristic $\chi(\bar{Z}) = 3$ and Kodaira dimension $\kappa(\bar{Z}) = 1$. By Proposition 8, $\bar{S}_0$ and $\bar{S}_1$ are two rational smooth curves on $\bar{Z}$ of self-intersection -3 meeting transversally. By the following two lemmata, this suffices to prove the theorem. □

Lemma 10. *Let $\mathcal{E}$ be a smooth minimal compact surface with $p_g(\mathcal{E}) = 2$, $\chi(\mathcal{E}) = 3$ and $\kappa(\mathcal{E}) = 1$. Suppose that there is a smooth irreducible rational curve C of self-intersection -3 lying on $\mathcal{E}$. Then:*

1. *The canonical map gives an elliptic fibration $f_{\mathrm{can}} : \mathcal{E} \to \mathbb{P}^1$;*
2. *C is a section of f_{can};*
3. *f_{can} has no multiple fibre.*

Proof. It follows from the Enriques–Kodaira classification of minimal surfaces that $\mathcal{E}$ admits an elliptic fibration $f : \mathcal{E} \to B$, where B is some smooth curve of genus g (cf. [1], p. 194). By Kodaira's formula for the canonical divisor of an elliptic surface (see Corollary V.12.3 of [1]),

$$\begin{aligned} K &\equiv \big(\chi(\mathcal{E}) - 2\chi(B)\big)F + \sum(m_i - 1)F_i \\ &= (1+2g)F + \sum(m_i-1)F_i, \end{aligned} \tag{1}$$

where F is any elliptic fibre, the sum is over all singular fibres F_i of multiplicity m_i and $\equiv$ denotes algebraic equivalence.

By the adjunction formula, $C \cdot K = 1$; thus, if $d = C \cdot F$, equation (1) yields

$$\begin{aligned} 1 = C \cdot K &= C \cdot \Big((1+2g)F + \sum(m_i-1)F_i\Big) \\ &= d\left(1 + 2g + \sum(m_i - 1)\right). \end{aligned} \tag{2}$$

Since g, d and m_i are all non-negative integers, (2) holds if only if $d = 1$ and $2g + \sum(m_i - 1) = 0$. This proves that C is a section for f, that $g = 0$ and that f has no multiple fibres.

Since the geometric genus of $\mathcal{E}$ is 2, the canonical map is a rational map $f_{\mathrm{can}} : \mathcal{E} \to \mathbb{P}^1$. Since $B = \mathbb{P}^1$, (1) becomes $K \sim F$. Thus, $f_{\mathrm{can}} = f$ up to an automorphism of $\mathbb{P}^1$. $\square$

Lemma 11. *Let B be a curve defined over a field K of characteristic 0 and let $\mathcal{E} \to B$ be a relatively minimal elliptic fibration defined over K which has two distinct sections C_0 and C_1 that meet. Let E be the elliptic curve over the function field $\kappa(B)$ of B which corresponds to (the generic fibre of) $(\mathcal{E}, C_0)$. Then the point Q of E corresponding to the section C_1 has infinite order.*

Proof. Let $t_0 \in B$ be a point over which C_0 and C_1 meet, let R be the local ring of t_0 on B and k its residue field. By Theorem IV.6.1 of [18], the special fibre of the Néron model $\mathcal{E}'/R$ of $E/K(B)$ is the curve obtained from the fibre $\mathcal{E}_{t_0}$ by removing all singular points. In particular, C_1 belongs to the kernel $\mathcal{E}_1$ of the reduction map (i.e., the specialization map at t_0): $\mathcal{E}'/R \to \tilde{\mathcal{E}}'/k$. Now, by Corollary IV.9.2 of [18], $\mathcal{E}_1$ is isomorphic to the kernel E_1 of the reduction map of a minimal Weierstrass model of E (see Proposition VII.2.2 of [17]), which, since the ground field has characteristic 0, has no non-trivial torsion by Proposition IV.3.2b of [17]. Therefore, Q has infinite order. $\square$

3 Rational models

3.1 The Galois action on $X(N)$

The purpose of this section is to show that the surfaces Z, $\tilde{Z}$ and $\bar{Z}$ have natural models defined over $\mathbb{Q}$ and that the fibration and its sections which were defined in the previous section are actually rational over $\mathbb{Q}$.

As a first step, let us recall some facts about the Galois action on $X(N)$, following §6.2 of Shimura [16], particularly Theorem 6.6 and Proposition 6.9.

For each positive integer N, let X_N denote the smooth projective curve over $\mathbb{Q}$ whose function field is the field $\mathcal{F}_N = \mathbb{Q}(j, f_{r,s})$ of modular functions of level N. Here j is the modular j-invariant which induces the isomorphism $j : X(1) \xrightarrow{\sim} \mathbb{P}^1_{\mathbb{C}}$, and the $f_{r,s} = f_{(r,s)}$ are the Fricke functions for $(r, s) \in \mathbb{Z}/N\mathbb{Z} \times \mathbb{Z}/N\mathbb{Z}$; cf. Lang [13], p. 65ff or Shimura [16], p. 137. If $\tilde{G}_N = \mathrm{GL}_2(\mathbb{Z}/N\mathbb{Z})/\pm\mathbf{1}$, then we have a natural $\tilde{G}_N$-action on $\mathcal{F}_N$ and hence also on X_N via the rule

$$g^* f_{r,s} = f_{(r,s)g}.$$

The induced action on the subfield $\mathbb{Q}_N := \mathbb{Q}(\zeta_N) \subset \mathcal{F}_N$ is via the determinant, i.e. we have $g^*{}_{|\mathbb{Q}_N} = \sigma^*_{\det(g)}$, for all $g \in \tilde{G}_N$. Here, for any $a \in (\mathbb{Z}/N\mathbb{Z})^\times$, $\sigma^*_a \in \mathrm{Aut}(\mathbb{Q}_N)$ is the unique automorphism such that $\sigma^*_a(\zeta) = \zeta^a$, for any N-th root of unity $\zeta \in \mathbb{Q}_N$.

Thus, if $p_N : X_N \to \mathrm{Spec}(\mathbb{Q}_N)$ denotes the structure map induced by the inclusion $\mathbb{Q}_N \subset \mathcal{F}_N$, then we have

$$p_N \circ g = \sigma_{\det(g)} \circ p_N, \quad \text{for all } g \in \tilde{G}_N. \tag{3}$$

Note that since the fixed field of $\tilde{G}_N$ is $\mathcal{F}_N^{\tilde{G}_N} = \mathbb{Q}(j)$, the quotient of X_N with respect to $\tilde{G}_N$ is

$$X_{\mathbb{Q}}(1) := \tilde{G}_N \backslash X_N \simeq \mathbb{P}^1_{\mathbb{Q}}.$$

Next, consider the subgroup

$$H_N = \{\pm \left(\begin{smallmatrix} 1 & 0 \\ 0 & d \end{smallmatrix}\right) : d \in (\mathbb{Z}/N\mathbb{Z})^\times\}/\{\pm 1\} \le \tilde{G}_N,$$

and let $F_N = \mathcal{F}_N^{H_N}$ be its fixed field. Since $H_N \cdot G_N = \tilde{G}_N$ and $H_N \cap G_N = \{1\}$ (and since $\mathbb{Q}_N$ is algebraically closed in $\mathcal{F}_N$), we have the following diagram of *linearly disjoint* field extensions:

$$\begin{tikzcd}
 & & \mathcal{F}_N \cdot \mathbb{C} \\
 & \mathcal{F}_N \arrow[ur, dash] \arrow[dd, dash, "G_N"] & \\
F_N \arrow[ur, dash, "H_N"] \arrow[dd, dash] & & \mathbb{C}(j) \arrow[uu, dash] \arrow[dd, dash] \\
 & F_1(\zeta_N) \arrow[ur, dash] \arrow[dd, dash] & \\
F_1 \arrow[ur, dash] \arrow[dd, dash] & & \mathbb{C} \\
 & \mathbb{Q}(\zeta_N) \arrow[ur, dash] & \\
\mathbb{Q} \arrow[ur, dash] & &
\end{tikzcd}$$

Thus, if we let

$$\pi_{\mathbb{Q}} = \pi_{\mathbb{Q},N} : X_{\mathbb{Q}}(N) := H_N \backslash X_N \to X_{\mathbb{Q}}(1) := \tilde{G}_N \backslash X_N$$

be the map induced on the quotient curves via the inclusion $H_N \subset \tilde{G}_N$, then the curve $X_{\mathbb{Q}}(N)$ (called *Shimura's canonical model* of $X(N)$) is absolutely irreducible over $\mathbb{Q}$, for we have that $X_{\mathbb{Q}}(N) \otimes \mathbb{C} = X(N)$ and $\pi_{\mathbb{Q}} \otimes \mathbb{C} = \pi$. More precisely, the above field diagram translates into the following *cartesian* diagram of curves:

$$\begin{tikzcd}
X_{\mathbb{Q}}(N) \arrow[d, "\pi_{\mathbb{Q}}"'] & X_N \arrow[l, "q_{X(N)}"'] \arrow[d, "\pi_{\mathbb{Q}_N}"] & X(N) \arrow[l] \arrow[d, "\pi"] \\
X_{\mathbb{Q}}(1) \arrow[d, "p_{\mathbb{Q}}"'] & X_{\mathbb{Q}_N}(1) \arrow[l, "q_{X(1)}"'] \arrow[d, "p_{\mathbb{Q}_N}"] & X(1) \arrow[l] \arrow[d] \\
\mathrm{Spec}(\mathbb{Q}) & \mathrm{Spec}(\mathbb{Q}_N) \arrow[l, "q"'] & \mathrm{Spec}(\mathbb{C}) \arrow[l]
\end{tikzcd}$$

Remark 12. Note that q, $q_{X(1)}$ and $q_{X(N)}$ are Galois covers with Galois group $\simeq (\mathbb{Z}/N\mathbb{Z})^\times$ and that $\pi_{\mathbb{Q}_N}$ is a (ramified) cover with covering group G_N. The action of G_N does not descend to $X_\mathbb{Q}(N)$, since G_N does not normalize H_N. On the other hand, the diagonal (Cartan) subgroup of $\tilde{G}_N$ does normalize H_N, so that its action descends to $X_\mathbb{Q}(N)$. In particular, the *diamond operator* τ_k acts on $X_\mathbb{Q}(N)$.

3.2 A $\mathbb{Q}$-rational model for $Z_{N,1}$

We now use Shimura's canonical model $X_\mathbb{Q}(N)/\mathbb{Q}$ (and the modular curve $X_N/\mathbb{Q}_N$) to construct a $\mathbb{Q}$-rational model $Z_\mathbb{Q}$ of the surface $Z = Z_{N,1}$. More precisely, we shall construct $Z_\mathbb{Q}$ as a suitable quotient of the surface $Y_{N,1} := X_N \times_{\mathbb{Q}_N} X_N$ and show that $Y_\mathbb{Q}(N) := X_\mathbb{Q}(N) \times X_\mathbb{Q}(N)$ maps to $Z_\mathbb{Q}$. To this end we first show:

Proposition 13. *The surface $Y_{N,1} := X_N \times_{\mathbb{Q}_N} X_N$ is naturally an irreducible component of $Y_N := X_N \times_\mathbb{Q} X_N$, and its stabilizer via the $\tilde{G}_N \times \tilde{G}_N$-action on Y_N is*

$$\mathrm{Stab}_{\tilde{G}_N \times \tilde{G}_N}(Y_{N,1}) = G := \{(g_1, g_2) \in \tilde{G}_N \times \tilde{G}_N : \det g_1 = \det g_2\}.$$

Moreover, we have

$$(p_N \times p_N) \circ g = \sigma_{\det g_i} \circ (p_N \times p_N), \quad \text{if } g = (g_1, g_2) \in G. \tag{4}$$

Furthermore, the base change maps $q_{Y(N)} : Y_{N,1} \to Y_\mathbb{Q}(N) := X_\mathbb{Q}(N) \times X_\mathbb{Q}(N)$ and $q_{Y(1)} : Y_{1,1} \to Y_\mathbb{Q}(1) := X_\mathbb{Q}(1) \times X_\mathbb{Q}(1)$ are Galois covers with covering groups $H := \{(h,h) : h \in H_N\} \leq G$ and $\bar{H} := G/(G_N \times G_N) \simeq H \simeq H_N$, respectively.

Proof. Put $Y = Y_{N,1}$ and let $pr_{Y,i}$ (resp. $pr_{Y_N,i}$) denote the projection onto the i-th factor of Y (resp. Y_N). Then there is a unique morphism $f = f_{N,1} : Y \to Y_N$ such that $pr_{Y_N,i} \circ f = pr_{Y,i}$. Clearly, f is a closed immersion. Now Y is irreducible because it is (smooth and) geometrically irreducible over $\mathrm{Spec}(\mathbb{Q}_N)$ (because $X_N/\mathbb{Q}_N$ is), and hence is a component of Y_N since both have dimension 2.

Now let $g = (g_1, g_2) \in \tilde{G}_N \times \tilde{G}_N$. Then $g \in \mathrm{Stab}(Y)$ if and only if g factors over f, i.e. if and only $p_N \circ g_1 = p_N \circ g_2$. Now by equation (3) we have $p_N \circ g_i = \sigma_{\det(g_i)} \circ p_N$, and so we see that g factors over f if and only $\sigma_{\det(g_1)} \circ p_N = \sigma_{\det(g_2)} \circ p_N$, and this is equivalent to $\det(g_1) = \det(g_2)$, i.e.

to $g \in G$. This proves the formula for the stabilizer and equation (4) follows immediately.

Next we observe that since $X_N = X_{\mathbb{Q}}(N) \otimes \mathbb{Q}_N$, we have the *cartesian diagram*

$$\begin{array}{ccc} Y_{\mathbb{Q}}(N) & \overset{q_{Y(N)}}{\longleftarrow} & Y \\ {\scriptstyle p\times p}\downarrow & & \downarrow {\scriptstyle p_N \times p_N} \\ \mathrm{Spec}(\mathbb{Q}) & \overset{q}{\longleftarrow} & \mathrm{Spec}(\mathbb{Q}_N) \end{array}$$

in which $p = p_{\mathbb{Q}} \circ \pi_{\mathbb{Q}} : X_{\mathbb{Q}}(N) \to \mathrm{Spec}(\mathbb{Q})$ is the structure map and $q_{Y(N)}$ is the unique morphism such that $pr_{Y_{\mathbb{Q}},i} \circ q_{Y(N)} = q_{X(N)} \circ pr_{Y,i}$, for $i = 1, 2$. (Here, $pr_{Y_{\mathbb{Q}},i} : Y_{\mathbb{Q}}(N) \to X_{\mathbb{Q}}(N)$ denotes the projection onto the i-th factor of $Y_{\mathbb{Q}}(N)$.)

Now since q is a Galois cover with group $\{\sigma_a\} \simeq (\mathbb{Z}/N\mathbb{Z})^{\times}$, the same is true for $q_{Y(N)}$; more precisely, $q_{Y(N)}$ is Galois with covering group $\{\tilde{\sigma}_a\}$, where $\tilde{\sigma}_a \in \mathrm{Aut}(Y)$ is the unique automorphism such that $q_{Y(N)} \circ \tilde{\sigma}_a = q_{Y(N)}$ and $(p_N \times p_N) \circ \tilde{\sigma}_a = \sigma_a \circ (p_N \times p_N)$. We observe:

$$\tilde{\sigma}_a = (h_a, h_a), \quad \text{where } h_a = \left(\begin{smallmatrix} 1 & 0 \\ 0 & a \end{smallmatrix}\right) \in H_N. \tag{5}$$

Indeed, by (4) we have $(p_N \times p_N) \circ (h_a, h_a) = \sigma_a \circ (p_N \times p_N)$. Moreover, since $q_{X(N)} \circ h = q_{X(N)}$ for all $h \in H_N$, we see that $pr_{Y_{\mathbb{Q}},i} \circ q_{Y(N)} \circ (h_a, h_a) = q_{X(N)} \circ pr_{Y,i} \circ (h_a, h_a) = q_{X(N)} \circ h_a \circ pr_{Y,i} = q_{X(N)} \circ pr_{Y,i}$, and so $q_{Y(N)} \circ (h_a, h_a) = q_{Y(N)}$ by the defining property of $q_{Y(N)}$. Thus, (h_a, h_a) satisfies the defining property of $\tilde{\sigma}_a$, and so (5) holds. We thus see that $Y_{\mathbb{Q}}(N)$ is the quotient of Y with respect to the subgroup H.

Clearly, $Y_{\mathbb{Q}_N}(1) := X_{\mathbb{Q}_N}(1) \times_{\mathbb{Q}_N} X_{\mathbb{Q}_N}(1)$ is the quotient of Y with respect to the subgroup $G_N \times G_N \le G$ with quotient map $\pi_{\mathbb{Q}_N} \times \pi_{\mathbb{Q}_N}$. Now since $G_N \lhd \tilde{G}_N$, we have that $G_N \times G_N \lhd G$, and hence $\bar{H} = G/(G_N \times G_N)$ acts as a group of automorphisms on $Y_{\mathbb{Q}_N}(1)$. Now the quotient map induces an isomorphism $H \xrightarrow{\sim} \bar{H}$ because $H \cap (G_N \times G_N) = \{1\}$ and $H \cdot (G_N \times G_N) = G$, and so by a similar argument as above we see that $q_{Y(1)} : Y_{\mathbb{Q}_N}(1) \to Y_{\mathbb{Q}}(1)$ is the quotient map with covering group $\bar{H}$. □

Theorem 14. *Let $\tilde{\Delta} = \Delta \cdot H = \{(g, g) : g \in \tilde{G}_N\} \le G$, where as before $\Delta = \{(g, g) : g \in G_N\}$. Then the quotient variety $Z_{\mathbb{Q}} := \tilde{\Delta}\backslash Y_{N,1}$ is a $\mathbb{Q}$-rational model of Z, and we have morphisms*

$$X_{\mathbb{Q}}(N) \times X_{\mathbb{Q}}(N) \xrightarrow{\Phi_{\mathbb{Q}}} Z_{\mathbb{Q}} \xrightarrow{\Psi_{\mathbb{Q}}} X_{\mathbb{Q}}(1) \times X_{\mathbb{Q}}(1) \tag{6}$$

such that the base change of $\Phi_{\mathbb{Q}}$ and $\Psi_{\mathbb{Q}}$ with $\mathbb{C}$ is Φ and Ψ. In particular, $\Psi_{\mathbb{Q}} \circ \Phi_{\mathbb{Q}} = \pi_{\mathbb{Q}} \times \pi_{\mathbb{Q}}$.

Proof. As before, write $Y = Y_{N,1}$. Furthermore, let

$$\pi_{\Delta} : Y \to Z_{\mathbb{Q}_N} := \Delta\backslash Y \quad \text{and} \quad \pi_{\tilde{\Delta}} : Y \to Z_{\mathbb{Q}} := \tilde{\Delta}\backslash Y$$

denote the associated quotient maps and spaces; these exist (as varieties) since we are dealing with quotients of (quasi-) projective varieties by finite groups.

Since $\Delta \triangleleft \tilde{\Delta}$, and $H \xrightarrow{\sim} \tilde{\Delta}/\Delta$, we see that $\pi_{\tilde{\Delta}} = q_{Z(N)} \circ \pi_{\Delta}$, where $q_Z : Z_{\mathbb{Q}_N} \to Z_{\mathbb{Q}}$ is the quotient map with covering group $\tilde{\Delta}/\Delta \simeq H$. Furthermore, the inclusions of subgroups $H \le \tilde{\Delta} \le G$ induce quotient maps $\Phi_{\mathbb{Q}} : Y_{\mathbb{Q}}(N) = H\backslash Y \to Z_{\mathbb{Q}} = \tilde{\Delta}\backslash Y$ and $\Psi_{\mathbb{Q}} : Z_{\mathbb{Q}} = \tilde{\Delta}\backslash Y \to Y_{\mathbb{Q}}(1) = G\backslash Y$ which fit into the following *cartesian diagram*:

$$\begin{array}{ccccc}
Y_{\mathbb{Q}}(N) & \xleftarrow{q_{Y(N)}} & Y & \longleftarrow & X(N) \times X(N) \\
{\scriptstyle \Phi_{\mathbb{Q}}} \downarrow & & \downarrow {\scriptstyle \pi_{\Delta}} & & \downarrow {\scriptstyle \Phi} \\
Z_{\mathbb{Q}} & \xleftarrow{q_Z} & Z_{\mathbb{Q}_N} & \longleftarrow & Z \\
{\scriptstyle \Psi_{\mathbb{Q}}} \downarrow & & \downarrow & & \downarrow {\scriptstyle \Psi} \\
Y_{\mathbb{Q}}(1) & \xleftarrow{q_{Y(1)}} & Y_{\mathbb{Q}_N}(1) & \longleftarrow & X(1) \times X(1) \\
\downarrow & & \downarrow & & \downarrow \\
\mathrm{Spec}(\mathbb{Q}) & \xleftarrow{q} & \mathrm{Spec}(\mathbb{Q}_N) & \longleftarrow & \mathrm{Spec}(\mathbb{C})
\end{array}$$

Thus, the base change of $\Phi_{\mathbb{Q}}$ and $\Psi_{\mathbb{Q}}$ is Φ and Ψ, respectively. Furthermore, we have $\Psi_{\mathbb{Q}} \circ \Phi_{\mathbb{Q}} = \pi_{\mathbb{Q}} \times \pi_{\mathbb{Q}}$ because we have equality for these morphisms after (faithfully flat) base change with q, and so they must be equal. $\square$

Remark 15. The above proof shows that $Z = Z_{N,1}$ has a canonical $\mathbb{Q}$-rational model $Z_{\mathbb{Q}} = Z_{N,1/\mathbb{Q}}$; this is the only case required here. In a similar way, however, one can show that every $Z_{N,\varepsilon}$ has a canonical $\mathbb{Q}$-rational model $Z_{N,\varepsilon/\mathbb{Q}}$. Indeed, we can use essentially the same construction if we replace $Y = Y_{N,1}$ by $Y_{N,\varepsilon} := X_N \times_{\mathbb{Q}_N,\sigma_\varepsilon} X_N$, the fibre product of X_N with itself via the morphisms $p_N : X_N \to \mathrm{Spec}(\mathbb{Q}_N)$ and $\sigma_\varepsilon \circ p_N$. In addition, the group Δ has to be replaced by the twisted diagonal subgroup $\Delta_\varepsilon = (1 \times h_\varepsilon^{-1})\Delta(1 \times h_\varepsilon) = \{(g, \alpha_\varepsilon(g)) : g \in G_N\}$, and similarly, $\tilde{\Delta}$ by $\tilde{\Delta}_\varepsilon = \Delta_\varepsilon H$. (Note that $\tilde{\Delta}_\varepsilon \leq G$ and that the group G still acts on $Y_{N,\varepsilon}$.) Thus, the canonical $\mathbb{Q}$-rational model of $Z_{N,\varepsilon}$ is

$$Z_{N,\varepsilon/\mathbb{Q}} = \tilde{\Delta}_\varepsilon \backslash Y_{N,\varepsilon}.$$

We further observe that each $Y_{N,\varepsilon}$ has a canonical embedding $f_\varepsilon : Y_{N,\varepsilon} \to Y_N := X_N \times_\mathbb{Q} X_N$, which leads to the decomposition of Y_N into its irreducible components:

$$Y_N := X_N \times_\mathbb{Q} X_N = \coprod_\varepsilon Y_{N,\varepsilon}; \tag{7}$$

note that $(1 \times h_\varepsilon^{-1}) \circ f_1 = f_\varepsilon$, so $Y_{N,\varepsilon} \simeq Y_{N,1}$ and $\tilde{G} := \tilde{G}_N \times \tilde{G}_N$ acts transitively on the components. In fact, since $G \triangleleft \tilde{G}$, we see that $\mathrm{Stab}_{\tilde{G}}(Y_{N,\varepsilon}) = G$ for all ε and hence $g(Y_{N,\varepsilon}) = Y_{N,a\varepsilon}$, where $a = \det(g_1)/\det(g_2)$ if $g = (g_1, g_2) \in \tilde{G}_N \times \tilde{G}_N$.

Proposition 16. *Every Hecke curve T_n on $Z_\mathbb{Q}$ is defined over $\mathbb{Q}$.*

Proof. Recall that $T_n = \Phi\left((\tau_k^{-1} \times \mathbf{1})T'(1,n)\right)$, where we have $k^2 n \equiv 1 \mod N$. By Proposition 7.7 of [16], $T'(1,n)$ is defined over $\mathbb{Q}$, i.e. we can view $T'(1,n) \subset X_\mathbb{Q}(N) \times X_\mathbb{Q}(N)$. By Remark 12, the action of τ_k commutes with the action of $\mathrm{Gal}(\bar{\mathbb{Q}}/\mathbb{Q})$, i.e. τ_k is defined over $\mathbb{Q}$, and hence $\Phi_\mathbb{Q}\left((\tau_k^{-1} \times \mathbf{1})T'(1,n)\right)$ is a model for T_n over $\mathbb{Q}$. $\square$

3.3 A model for the elliptic fibration

We now return to the situation of §2, i.e. we assume that $N = 11$. Here we have:

Proposition 17. *The surface $\tilde{Z}$ admits a rational model $\tilde{Z}_\mathbb{Q}$. Moreover, each component of E_∞ is defined over $\mathbb{Q}$.*

Proof. By the uniqueness property of the *minimal* resolution of singularities, the morphism $\sigma : \tilde{Z} \to Z$ descends to a morphism $\sigma_\mathbb{Q} : \tilde{Z}_\mathbb{Q} \to Z_\mathbb{Q}$. This proves the first part.

Since Ψ is defined over $\mathbb{Q}$, the set Σ_∞ is Galois invariant. By Proposition 4.4, we see that each singularity of Σ_∞ has a unique type. Since the singularity type is a Galois invariant, it follows that every singularity z_i of

Σ_∞ is $\mathbb{Q}$-rational. Since σ is defined over $\mathbb{Q}$, the chain $E_{\infty,i}$ is $\mathbb{Q}$-rational. It is clear that $\tilde{C}_{\infty,1}$ is $\mathbb{Q}$-rational as well. Therefore, the component of $E_{\infty,i}$ which meets $\tilde{C}_{\infty,1}$ (which is unique by Proposition 5) is $\mathbb{Q}$-rational, and hence so are the other components. This proves the second part. $\square$

Proposition 18. *The surface $\bar{Z}$ admits a $\mathbb{Q}$-rational model $\bar{Z}_{\mathbb{Q}}$. If f_{can} is the canonical map of $\bar{Z}_{\mathbb{Q}}$, then $f_{\mathrm{can}} : Z_{\mathbb{Q}} \to \mathbb{P}^1_{\mathbb{Q}}$ is an elliptic fibration which admits the sections $\bar{S}_0$ and $\bar{S}_1$.*

Proof. Although this statement could be proved by applying the Minimal Model Theorem of Shafarevich–Lichtenbaum to the canonical map of $\tilde{Z}_{\mathbb{Q}}$, we prefer to give the following more explicit proof.

Recall from Proposition 7(b), that $\bar{Z}$ is obtained from $\tilde{Z}$ by blowing down $\tilde{T}_1$, Γ_0, Γ_2; $\tilde{T}_3$; $\tilde{T}_4$. We claim that all of these curves are $\mathbb{Q}$-rational.

It follows from Propositions 16 and 17 that every $\tilde{T}_n$ is $\mathbb{Q}$-rational. Arguing as in the proof of Proposition 17, we conclude that E_0 and E_1 are $\mathbb{Q}$-rational. It follows that Γ_0 and Γ_1 are $\mathbb{Q}$-rational, since they are the unique components of E_0 and E_1 meeting $\tilde{T}_1$—cf. Proposition 7(a). This proves that $\bar{Z}$ is defined over $\mathbb{Q}$. Therefore, the canonical class of $\bar{Z}$ is $\mathbb{Q}$-rational, and thus f_{can} is defined over $\mathbb{Q}$.

Since S_0 and S_1 are the unique components of E_∞ of self-intersection -4, and they meet $\tilde{C}_{\infty,1}$ and $\tilde{C}_{\infty,2}$, respectively, it follows that they are fixed by the Galois action. Thus, their images $\bar{S}_0$ and $\bar{S}_1$ in $\bar{Z}_{\mathbb{Q}}$ are $\mathbb{Q}$-rational. $\square$

Notation. The set $M = M(Z_{N,1})$ of *Mazur's trivial points* of $Z = Z_{N,1}$ is defined by

$$M(Z_{N,1}) \;=\; \bigcup_n \Psi_{\mathbb{Q}}^{-1}\left(\xi_n\big(X_0'(n)(\mathbb{Q})\big)\right),$$

where $\xi_n : X_0(n) \to T'(1,n) \subset X(1) \times X(1)$ is the normalization map and $X_0'(n) := X_0(n) \setminus \{\text{cusps}\}$ is the *non-cuspidal part* of $X_0(n)$.

In addition, we put $\tilde{M} = \sigma^{-1}(M) \cap \tilde{Z}_{\mathbb{Q}}(\mathbb{Q})$ and let $\bar{M}$ denote the image of $\tilde{M}$ in $\bar{Z}_{\mathbb{Q}}$.

Theorem 19. *The canonical map $f_{\mathrm{can}} : \bar{Z}_{\mathbb{Q}} \to \mathbb{P}^1_{\mathbb{Q}}$ admits infinitely many sections $\{S_i\}$ such that $S_i(\mathbb{Q}) \setminus \bar{M}$ is infinite for every i.*

Proof. By Proposition 18, the elliptic curve $E/\mathbb{C}(t)$ of Theorem 9 is actually defined over $\mathbb{Q}$, as is the point of infinite order Q. Thus, the multiples of Q

correspond to infinitely many rational sections $\{S_i\}$ of f_{can}. Since the genus of $X_0(n)$ is ≥ 1 for $n \geq 16$, only finitely many sections can be components of some $\bar{\Psi}^*\xi_n(X_0(n))$. By restricting the index i, we can assume that no S_i is contained in $\bar{\Psi}^*\xi_n(X_0(n))$. By a theorem of Mazur and Kenku [11], $X_0'(n)(\mathbb{Q}) = \emptyset$ for $n > 163$. Thus, $\tilde{M}$ is contained in finitely many curves of $\tilde{Z}$, and each section S_i has a finite intersection with it. Since $S_i \simeq \mathbb{P}^1_{\mathbb{Q}}$, the theorem follows. $\square$

4 Modular Interpretation

4.1 Product moduli

Fix a positive integer N, and let $\mathcal{X}_N$ be the contravariant functor

$$\mathcal{X}_N : \underline{\mathrm{Sch}}_{/\mathbb{Q}} \longrightarrow \underline{\mathrm{Sets}}$$

from the category of schemes over $\mathbb{Q}$ to the category of sets which is defined as follows. If S is a $\mathbb{Q}$-scheme, then let $\mathcal{X}_N(S)$ be

$$\left\{\langle E/S, \alpha\rangle : E/S \text{ elliptic curve, } \alpha : E[N] \xrightarrow{\sim} (\mathbb{Z}/N\mathbb{Z} \times \mathbb{Z}/N\mathbb{Z})_{/S}\right\},$$

where $\langle\cdot\rangle$ denotes the class of S-isomorphisms, and if $f : T \to S$ is a morphism of $\mathbb{Q}$-schemes, then $\mathcal{X}_N(f) : \mathcal{X}_N(S) \to \mathcal{X}_N(T)$ is the map induced by base change, i.e. $\mathcal{X}_N(f)(\langle E/S, \alpha\rangle) = \langle E_{(T)}, \alpha_{(T)}\rangle$, where $E_{(T)} = E \times_S T$ and $\alpha_{(T)} = \alpha \times_S id_T : E_{(T)}[N] = E[N] \times_S T \to (\mathbb{Z}/N\mathbb{Z})^2_{/T} = (\mathbb{Z}/N\mathbb{Z})^2_{/S} \times_S T$.

We have a natural forget map $\boldsymbol{\pi}_N : \mathcal{X}_N \to \mathcal{X}_1$ defined by

$$\boldsymbol{\pi}_{N,S}(\langle E/S, \alpha\rangle) = \langle E/S\rangle;$$

here we use the obvious fact that the functor $\mathcal{X}_1$ can be identified with the functor that classifies isomorphism classes of elliptic curves. Clearly, $\boldsymbol{\pi}_N$ is $\tilde{G}_N$-invariant, where the group $\tilde{G}_N = \mathrm{GL}_2(\mathbb{Z}/N\mathbb{Z})/\pm\mathbf{1}$ acts on the left on $\mathcal{X}_N$ by $g \cdot \langle E/S, \alpha\rangle = \langle E/S, g \circ \alpha\rangle$. (Note that $\langle E/S, -\alpha\rangle = \langle E/S, \alpha\rangle$, so the action factors over the quotient group.)

It is well known (cf. [2], [3]) that the affine curve $X_N' = X_N \setminus \{\text{cusps}\}$, the non-cuspidal part of the curve $X_N/\mathbb{Q}$ introduced in subsection 3.1, represents the functor $\mathcal{X}_N$ when $N \geq 3$, i.e. for every $\mathbb{Q}$-scheme S we have a bijection

$$\mathcal{P}_{\mathcal{X}_N,S} : \mathcal{X}_N(S) \xrightarrow{\sim} X_N'(S),$$

which is compatible with base change. Moreover, this bijection is $\tilde{G}_N$-equivariant, i.e. we have $\mathcal{P}_{\mathcal{X}_N,S}(g\langle E/S,\alpha\rangle) = g\mathcal{P}_{\mathcal{X}_N,S}(\langle E/S,\alpha\rangle)$.

For $N \leq 2$ the curve X'_N only *coarsely* represents $\mathcal{X}_N$: we then still have the maps $\mathcal{P}_{\mathcal{X}_N,S}$, but they are only bijections when $S = \mathrm{Spec}(K)$, K an algebraically closed field. In the case $N = 1$ and $S = \mathrm{Spec}(K)$, K any field, $\mathcal{P}_{\mathcal{X}_1,K}$ can be given explicitly; it is the unique map such that the function $j \in \kappa(X_1) \simeq \mathbb{Q}(j)$ evaluates to the j-invariant $j(E/K)$ of the elliptic curve:

$$j(\mathcal{P}_{\mathcal{X}_1,K}(\langle E/K\rangle)) = j(E/K).$$

Note that the above $\tilde{G}_N$-equivariance of $\mathcal{P}_{\mathcal{X}_N}$ implies the compatibility relation

$$\mathcal{P}_{\mathcal{X}_1,K} \circ \boldsymbol{\pi}_{N,K} = \pi_N \circ \mathcal{P}_{\mathcal{X}_N,K},$$

where $\pi_N : X_N \to X_1 \simeq \tilde{G}_N \backslash X_N$ denotes the quotient morphism.

Recall from subsection 3.1 that X_N and hence also X'_N come equipped with the structure maps

$$p_N : X_N \to \mathrm{Spec}(\mathbb{Q}_N), \qquad p'_N : X'_N \to \mathrm{Spec}(\mathbb{Q}_N).$$

Viewing $\mathrm{Spec}(\mathbb{Q}_N)$ as the scheme which represents the functor μ_N^{prim} that associates to each scheme $S/\mathbb{Q}$ its set of primitive N-th roots of unity (i.e. the set of morphisms $\mathrm{Spec}(\mathbb{Q}_N) \to S$), we see that the morphism p'_N represents the morphism of functors $\boldsymbol{p}'_N : \mathcal{X}_N \to \mu_N^{prim}$ defined by

$$\boldsymbol{p}'_{N,S}(\langle E/S,\alpha\rangle) = e_N(\alpha^{-1}(1,0),\alpha^{-1}(0,1)) \in \mu_N^{prim}(S), \tag{8}$$

in which $e_N = e_N^E : E[N] \times E[N] \to \mathbb{G}_{m/S}$ denotes the e_N-pairing (cf. [15] or [10]).

Next, consider the product functor $\mathcal{Y}_N = \mathcal{X}_N \times \mathcal{X}_N$, as well as the subfunctor $\mathcal{Y}_{N,\varepsilon}$ of $\mathcal{Y}_N$ defined for $\varepsilon \in (\mathbb{Z}/N\mathbb{Z})^\times$ by

$$\begin{aligned} \mathcal{Y}_{N,\varepsilon}(S) \;=\; & \big\{\langle E_1/S,\alpha_1; E_2/S,\alpha_2\rangle \in \mathcal{Y}_N(S) : \\ & \quad e_N \circ \big((\alpha_2^{-1}\circ\alpha_1)\times(\alpha_2^{-1}\circ\alpha_1)\big) = e_N^{\varepsilon}\big\}; \end{aligned}$$

like $\mathcal{X}_N$, these are functors from $\underline{\mathrm{Sch}}_{/\mathbb{Q}}$ to $\underline{\mathrm{Sets}}$. We have:

Proposition 20. *If $N \geq 3$, the $\mathbb{Q}$-schemes $Y'_N = X'_N \times_{\mathbb{Q}} X'_N$ and $Y'_{N,1} = X'_N \times_{\mathbb{Q}_N} X'_N$ represent the functors $\mathcal{Y}_N$ and $\mathcal{Y}_{N,1}$, respectively; i.e. we have natural isomorphisms of functors*

$$\mathcal{P}_{\mathcal{Y}_N} : \mathcal{Y}_N \xrightarrow{\sim} h_{Y'_N} \quad \textit{and} \quad \mathcal{P}_{\mathcal{Y}_{N,1}} = \mathcal{P}_{\mathcal{Y}_N|\mathcal{Y}_{N,1}} : \mathcal{Y}_{N,1} \xrightarrow{\sim} h_{Y'_{N,1}}.$$

Proof. Since $\mathcal{Y}_N$ is just the product functor, the first assertion is obvious. For the second notice that the condition that $e_N^{E_1} = e_N^{E_2} \circ (\alpha_2 \times \alpha_2)^{-1} \circ (\alpha_1 \times \alpha_1)$ is by equation (8) equivalent to the condition that $\boldsymbol{p}'_N(\langle E_1, \alpha_1\rangle) = \boldsymbol{p}'_N(\langle E_2, \alpha_2\rangle)$, which means that $\mathcal{Y}_{N,1} = \mathcal{X}_N \times_{\mathbb{Q}_N} \mathcal{X}_N$ is the fibre product of $\mathcal{X}_N$ with itself over $\mathrm{Spec}(\mathbb{Q}_N)$ via $\boldsymbol{p}'_N$, and hence is represented by the fibre product $Y'_{N,1} = X'_N \times_{\mathbb{Q}_N} X'_N$ over $\mathrm{Spec}(\mathbb{Q}_N)$ (viewed as a $\mathbb{Q}$-scheme). □

Remark 21. The same argument shows that $\mathcal{Y}_{N,\varepsilon} = \mathcal{X}_N \times_{\mathbb{Q}_N,\sigma_\varepsilon} \mathcal{X}_N$ is the fibre product of $\mathcal{X}_N$ with itself via the maps $\boldsymbol{p}'_N$ and $\sigma_\varepsilon \circ \boldsymbol{p}'_N$, and hence is represented by the scheme $Y'_{N,\varepsilon} = X'_N \times_{\mathbb{Q}_N,\sigma_\varepsilon} X'_N$ (cf. Remark 15). Thus, $\mathcal{P}_{\mathcal{Y}_N}$ restricts to an isomorphism

$$\mathcal{P}_{\mathcal{Y}_{N,\varepsilon}} = \mathcal{P}_{\mathcal{Y}_N|\mathcal{Y}_{N,\varepsilon}} : \mathcal{Y}_{N,\varepsilon} \xrightarrow{\sim} h_{Y'_{N,\varepsilon}}.$$

Note that although $Y'_{N,\varepsilon}$ is a scheme over $\mathbb{Q}_N$, we view it here as a scheme over $\mathbb{Q}$; in particular, $Y'_{N,\varepsilon}/\mathbb{Q}$ is not geometrically connected.

4.2 Quotient moduli

Let $\mathcal{Z}_N$ be the contravariant functor of $\mathbb{Q}$-schemes defined by

$$\begin{aligned}\mathcal{Z}_N(S) \;=\; \big\{&\langle E_1/S, E_2/S, \psi\rangle : \\ &E_1/S, E_2/S \text{ elliptic curves}, \psi : E_1[N] \xrightarrow{\sim} E_2[N]\big\}.\end{aligned}$$

We have natural maps of functors $\boldsymbol{\Phi}_N : \mathcal{Y}_N \to \mathcal{Z}_N$ and $\boldsymbol{\Psi} : \mathcal{Z}_N \to \mathcal{Y}_1$ defined for each $\mathbb{Q}$-scheme S by the rules

$$\begin{aligned}\boldsymbol{\Phi}_{N,S}(\langle E_1, \alpha_1; E_2, \alpha_2\rangle) &= \langle E_1, E_2, \alpha_2^{-1} \circ \alpha_1\rangle,\\ \boldsymbol{\Psi}_S(\langle E_1, E_2, \psi\rangle) &= \langle E_1, E_2\rangle.\end{aligned}$$

Clearly, $\boldsymbol{\Psi} \circ \boldsymbol{\Phi}_N = \boldsymbol{\pi}_N \times \boldsymbol{\pi}_N$ while $\boldsymbol{\Phi}_N$ is $\tilde{G}_N$-invariant with respect to the diagonal action on $\mathcal{Y}_N$, and so $\boldsymbol{\Phi}_N$ factors over the quotient functor $\boldsymbol{\Pi}_N : \mathcal{Y}_N \to \overline{\mathcal{Y}}_N := \tilde{G}_N\backslash\mathcal{Y}_N$, i.e. we have an induced map

$$\overline{\boldsymbol{\Phi}}_N : \overline{\mathcal{Y}}_N := \tilde{G}_N\backslash\mathcal{Y}_N \to \mathcal{Z}_N$$

such that $\boldsymbol{\Phi}_N = \overline{\boldsymbol{\Phi}}_N \circ \boldsymbol{\Pi}_N$. It is easy to see that $\overline{\boldsymbol{\Phi}}_N$ is an injection. Unfortunately, $\overline{\boldsymbol{\Phi}}_N$ is not bijective, so $\mathcal{Z}_N$ is not quite the quotient functor. (However, both functors have the same sheafifications in the étale topology). Nevertheless, $\mathcal{Z}_N$ still is *coarsely represented* by the quotient scheme $Z'_N := \tilde{G}_N\backslash Y'_N$, the non-cuspidal part of $Z_N := \tilde{G}_N \backslash Y_N$. This means that we have a natural map (of functors) $\mathcal{P}_{\mathcal{Z}_N} : \mathcal{Z}_N \to h_{Z'_N}$, where $h_{Z'_N}$ denotes the functor associated to the $\mathbb{Q}$-scheme Z'_N (i.e. $h_{Z'_N}(S) = Z'_N(S) = \mathrm{Hom}_{\mathrm{Sch}}(S, Z'_N)$), which is bijective on geometric points and which is "best possible" in a certain sense. (In particular, it then follows that the above functor $\mathbf{\Phi}_N : \mathcal{Y}_N \to \mathcal{Z}_N$ is compatible with the quotient morphism $\Phi_N : Y'_N \to \tilde{G}_N \backslash Y'_N = Z'_N$.) Since the proof of this general fact is somewhat technical (cf. [7]), we content ourselves with the following result which suffices for our purposes.

Proposition 22. *For every field $K \supset \mathbb{Q}$ there is a* unique *map*

$$\mathcal{P}_{\mathcal{Z}_N,K} : \mathcal{Z}_N(K) \to Z'_N(K)$$

which is compatible with base change (of fields) such that the diagram

$$\begin{array}{ccc} \mathcal{Y}_N(K) & \stackrel{\mathcal{P}_{\mathcal{Y}_N,K}}{\longrightarrow} & Y'_N(K) \\ {\scriptstyle \mathbf{\Phi}_{N,K}} \downarrow & & \downarrow {\scriptstyle \Phi_N} \\ \mathcal{Z}_N(K) & \stackrel{\mathcal{P}_{\mathcal{Z}_N,K}}{\longrightarrow} & Z'_N(K) \\ {\scriptstyle \mathbf{\Psi}_K} \downarrow & & \downarrow {\scriptstyle \Psi} \\ \mathcal{Y}_1(K) & \stackrel{\mathcal{P}_{\mathcal{Y}_1,K}}{\longrightarrow} & Y'_1(K) \end{array} \tag{9}$$

commutes. Furthermore, $\mathcal{P}_{\mathcal{Z}_N,K}$ is a bijection if K is algebraically closed.

Proof. Suppose first that $K = \overline{K}$ is algebraically closed. Then the map $\overline{\mathbf{\Phi}}_{N,K} : \overline{\mathcal{Y}}_N(K) := \tilde{G}_N \backslash \mathcal{Y}_N(K) \to \mathcal{Z}_N(K)$ is bijective.

Indeed, since we already know that $\overline{\mathbf{\Phi}}_{N,K}$ is injective, it is enough to show that $\mathbf{\Phi}_{N,K}$ (and hence $\overline{\mathbf{\Phi}}_{N,K}$) is surjective. For this, let $\langle E_1, E_2, \psi \rangle \in \mathcal{Z}_N(K)$. Since K is algebraically closed (and $\mathrm{char}(K) = 0$), there is a K-rational level N structure $\alpha_2 : E_2[N] \xrightarrow{\sim} \mathbb{Z}/N\mathbb{Z} \times \mathbb{Z}/N\mathbb{Z}$ on E_2. Put $\alpha_1 := \alpha_2 \circ \psi$. Then $\langle E_1, \alpha_1; E_2, \alpha_2 \rangle \in \mathcal{Y}_N(K)$ and $\mathbf{\Phi}_{N,K}(\langle E_1, \alpha_1; E_2, \alpha_2 \rangle) = \langle E_1, E_2, \psi \rangle$. This means that $\mathbf{\Phi}_{N,K}$ is surjective and so $\mathcal{Z}_N(K)$ is the $\tilde{G}_N$-quotient of $\mathcal{Y}_N(K)$ by $\mathbf{\Phi}_{N,K}$.

On the other hand, since $Z'_N = \tilde{G}_N \backslash Y'_N$ is the geometric quotient of Y'_N, we know (since K is algebraically closed) that $Z'_N(K)$ is the (set-theoretic) $\tilde{G}_N$-quotient of $Y'_N(K)$. Thus, since $\mathcal{P}_{\mathcal{Y}_N,K} : \mathcal{Y}_N(K) \to Y'_N(K)$ is bijective, it follows that $(\mathcal{Z}_N(K), \mathbf{\Phi}_{N,K})$ and $(Z'_N(K), \Phi_N \circ \mathcal{P}_{\mathcal{Y}_N,K})$ are both set-theoretic quotients of $\mathcal{Y}_N(K)$, so there is a unique bijection $\mathcal{P}_{\mathcal{Z}_N,K} : \mathcal{Z}_N(K) \xrightarrow{\sim} Z'_N(K)$

such that $\mathcal{P}_{\mathcal{Z}_N,K} \circ \mathbf{\Phi}_{N,K} = \Phi_N \circ \mathcal{P}_{\mathcal{Y}_N,K}$, i.e. such that the top part of diagram (9) commutes.

We observe that this bijection is $\mathrm{Aut}(K)$-equivariant, i.e. we have

$$\mathcal{P}_{\mathcal{Z}_N,K}(\langle E_1, E_2, \psi\rangle^\sigma) = \mathcal{P}_{\mathcal{Z}_N,K}(\langle E_1, E_2, \psi\rangle)^\sigma, \quad \text{for } \sigma \in \mathrm{Aut}(K).$$

Here σ acts (on the right) on $\mathcal{Z}_N(K)$ by functoriality (i.e. by $\mathcal{Z}_N(\sigma)$) and on $Z'(K)$ by the usual action on K-rational points.

To prove that the bottom square of diagram (9) commutes, observe that the outer rectangle of (9) commutes because $\mathbf{\Psi} \circ \mathbf{\Phi}_N = \boldsymbol{\pi}_N \times \boldsymbol{\pi}_N$, $\Psi \circ \Phi_N = \pi_N \times \pi_N$, and $\mathcal{P}_{\mathcal{X}_1,N} \circ \boldsymbol{\pi}_{N,K} = \pi_N \circ \mathcal{P}_{\mathcal{X}_N,K}$, and so the assertion follows by a diagram chase since $\mathbf{\Phi}_{N,K}$ is surjective (when K is algebraically closed).

Now consider the case of an arbitrary field K with algebraic closure $\overline{K}$ and let $G_K = \mathrm{Gal}(\overline{K}/K)$ denotes its absolute Galois group. Then we can identify $Z'_N(K)$ as the subset of G_K-invariant elements of $Z'_N(\overline{K})$, i.e. $Z'_N(K) = Z'_N(\overline{K})^{G_K}$. The inclusion $i^* : K \to \overline{K}$ induces a morphism $i : \mathrm{Spec}(\overline{K}) \hookrightarrow \mathrm{Spec}(K)$ and hence a map $\mathcal{Z}_N(i) : \mathcal{Z}_N(K) \to \mathcal{Z}_N(\overline{K})$. Now the image of $\mathcal{Z}_N(i)$ is actually G_K-invariant because $i \circ \sigma = i$, for all $\sigma \in G_K$, and so we can define $\mathcal{P}_{\mathcal{Z}_N,K}$ as the composition

$$\begin{aligned}\mathcal{P}_{\mathcal{Z}_N,K} = {\mathcal{P}_{\mathcal{Z}_N,\overline{K}}}^{G_K} \circ \mathcal{Z}_N(i) :& \\ &\mathcal{Z}_N(K) \to \mathcal{Z}_N(\overline{K})^{G_K} \to Z_N(\overline{K})^{G_K} = Z_N(K).\end{aligned}$$

It is then clear that the diagram (9) commutes and that the $\mathcal{P}_{\mathcal{Z}_N,K}$ commute with base change. Furthermore, $\mathcal{P}_{\mathcal{Z}_N,K}$ is unique, for compatibility with base change (which includes Galois invariance) forces the above definition. $\square$

Remark 23. The above proof shows that we have the following formula for $\mathcal{P}_{\mathcal{Z}_N,K}$:

$$\mathcal{P}_{\mathcal{Z}_N,K}(\langle E_1, E_2, \psi\rangle) = \Phi_N(\mathcal{P}_{\mathcal{Y}_N,\overline{K}}(\langle E_1 \otimes \overline{K}, \alpha_2 \circ \psi; E_2 \otimes \overline{K}, \alpha_2\rangle)),$$

in which $\alpha_2 : E_2[N]_{/\overline{K}} \to (\mathbb{Z}/N\mathbb{Z})^2$ is *any* level N-structure of $E_2 \otimes \overline{K}$.

Note that for a non-algebraically closed field K the map $\mathcal{P}_{\mathcal{Z}_N,K}$ is *not* injective. Indeed, for any $\langle E_1, E_2, \psi\rangle \in \mathcal{Z}_N(K)$ and any quadratic character $\chi : G_K \to \{\pm 1\}$ we have

$$\mathcal{P}_{\mathcal{Z}_N,K}(\langle E_1, E_2, \psi\rangle) = \mathcal{P}_{\mathcal{Z}_N,K}(\langle E_{1,\chi}, E_{2,\chi}, \psi_\chi\rangle),$$

where $E_{i,\chi} = (E_i)_\chi$ denotes the quadratic twist of E_i/K, and

$$\psi_\chi : E_{1,\chi}[N] \to E_{2,\chi}[N]$$

is the χ-twist of ψ, i.e. the unique isomorphism such that $\psi_\chi \otimes \overline{K} = f_2^{-1} \circ (\psi \otimes \overline{K}) \circ f_{1|E_\chi[N]}$, where $f_i : E_{i,\chi} \otimes \overline{K} \xrightarrow{\sim} E_i \otimes \overline{K}$ is the twist isomorphism associated to χ. (Thus, f_i is a $\overline{K}$-isomorphism such that $f_i(id_{E_{i,\chi}} \times \sigma) = \chi(\sigma)(id_{E_i} \times \sigma)$, for all $\sigma \in G_K$.) Note that it follows from the definition that $\psi_\chi \otimes \overline{K} \circ (id_{E_{1,\chi}} \times \sigma) = (id_{E_{2,\chi}} \times \sigma) \circ \psi_\chi$, so ψ_χ exists by descent theory.

However, we do have that $\mathcal{P}_{\mathcal{Z}_N,K}$ is always surjective. For simplicity, we prove the following slightly weaker assertion in which we replace Z'_N by the open subscheme $Z''_N := \Phi_N(X''_N \times X''_N)$, where $X''_N = X_N \setminus \pi_N^{-1}(\{\bar{P}_0, \bar{P}_1, \bar{P}_\infty\})$.

Proposition 24. *For every field K we have $Z''_N(K) \subset \mathrm{Im}(\mathcal{P}_{\mathcal{Z}_N,K})$.*

Before proving this, we first establish the following two facts.

Lemma 25. *Let $z \in Z'_N(K)$. Then there exist elliptic curves E_1/K and E_2/K and level N structures $\alpha_i : E_i[N]_{/\overline{K}} \xrightarrow{\sim} \mathbb{Z}/N\mathbb{Z} \times \mathbb{Z}/N\mathbb{Z}$ for $i = 1, 2$ such that*

$$\Phi_N(\mathcal{P}_{\mathcal{Y}_N,\overline{K}}(\langle E_1 \otimes \overline{K}, \alpha_1; E_2 \otimes \overline{K}, \alpha_2\rangle)) = z.$$

Proof. Since $\Phi_N : Y'_N \to Z'_N$ is a geometric quotient, there exists $y \in Y'_N(\overline{K})$ such that $\Phi_N(y) = z$. Then by Proposition 20 there are elliptic curves $E_i/\overline{K}$ and level N structures $\alpha_i : E_i[N] \to (\mathbb{Z}/N\mathbb{Z})^2$ such that $\mathcal{P}_{\mathcal{Y}_N}(\langle E_1/\overline{K}, \alpha_1; E_2/\overline{K}, \alpha_2\rangle) = y$.

Since $z \in Z'_N(K)$, we have that $\Psi(z) \in X'_1(K) \times X'_1(K) \simeq \mathbb{A}^1(K) \times \mathbb{A}^1(K)$. But $\Psi(z) = \Psi\Phi_N(y) = (j(E_1/\overline{K}), j(E_2/\overline{K}))$, so we see that $j(E_i/\overline{K}) \in K$. This means that there exist elliptic curves E'_i/K such that $E'_i \otimes \overline{K} \simeq E_i$. Taking these as representatives of the isomorphism class (and adapting the α_i accordingly) yields the assertion. ☐

Lemma 26. *Suppose that E_1 and E_2 are elliptic curves over a field $K \supset \mathbb{Q}$ and $\psi : E_1[N]_{/\overline{K}} \xrightarrow{\sim} E_2[N]_{/\overline{K}}$ is an isomorphism such that*

$$\mathcal{P}_{\mathcal{Z}_N}(\langle E_1 \otimes \overline{K}, E_2 \otimes \overline{K}, \psi\rangle) \in Z''_N(K).$$

Then there is a character $\chi : G_K \to \{\pm 1\}$ such that

$$\psi\sigma = \sigma\psi\chi(\sigma), \qquad \textit{for all } \sigma \in G_K. \tag{10}$$

Proof. Let $\alpha_2 : E_2[N]_{/\overline{K}} \to \mathbb{Z}/N\mathbb{Z} \times \mathbb{Z}/N\mathbb{Z}$ be a level N-structure and put $\alpha_1 = \alpha_2 \circ \psi$. Then, writing $E_i/\overline{K}$ in place of $E_i \otimes \overline{K}/\overline{K}$, we have $\mathbf{\Phi}_N(\langle E_1/\overline{K},\alpha_1; E_2/\overline{K},\alpha_2\rangle) = \langle E_1/\overline{K}, E_2/\overline{K}, \psi\rangle$ and thus, if we let

$$z = \mathcal{P}_{\mathcal{Z}_N}(\langle E_1/\overline{K}, E_2/\overline{K}, \psi\rangle) \text{ and } y = \mathcal{P}_{\mathcal{Y}_N}(\langle E_1/\overline{K}, \alpha_1; E_2/\overline{K}, \alpha_2\rangle),$$

then $\Phi_N(y) = z$. Since z is G_K-invariant, we have for any $\sigma \in G_K$ that $y^\sigma \in \Phi_N^{-1}(z)$, so $y^\sigma = g_\sigma \cdot y$, for some $g_\sigma \in \mathrm{GL}_2(\mathbb{Z}/N\mathbb{Z})$. Note that g_σ is unique up to $\pm\mathbf{1}$ because $\tilde{G}_N = \mathrm{GL}_2(\mathbb{Z}/N\mathbb{Z})/\pm\mathbf{1}$ acts freely on $\Phi_N^{-1}(z)$; here we use the fact that $z \in Z_N''(K)$.

On the moduli problem, this means that

$$\langle E_1/\overline{K}, \alpha_1; E_2/\overline{K}, \alpha_2\rangle^\sigma = g_\sigma \cdot \langle E_1/\overline{K}, \alpha_1; E_2/\overline{K}, \alpha_2\rangle.$$

Hence, since $E_1/\overline{K}$ and $E_2/\overline{K}$ are G_K-invariant,

$$\langle E_1/\overline{K}, \alpha_1\sigma; E_2/\overline{K}, \alpha_2\sigma\rangle = \langle E_1/\overline{K}, g_\sigma\alpha_1; E_2/\overline{K}, g_\sigma\alpha_2\rangle.$$

In other words, there are automorphisms $\chi_{i,\sigma}$ of $E_i/\overline{K}$ (which depend on the choice of g_σ), such that $g_\sigma\alpha_i\chi_{i,\sigma} = \alpha_i\sigma$, for $i = 1, 2$. Now since $z \in Z_N''(K)$, we have $j(E_i/\overline{K}) \neq 0, 1728$, so $\mathrm{Aut}(E_i/\overline{K}) = \{id_{E_i}\} \simeq \{\pm\mathbf{1}\}$, and hence $\chi_{i,\sigma} \in \{\pm 1\}$. By replacing g_σ with $-g_\sigma$ if necessary (and hence replacing $\chi_{i,\sigma}$ by $-\chi_{i,\sigma}$), we may suppose that $\chi_{2,\sigma} = 1$, for all $\sigma \in G_K$. Write $\chi(\sigma) = \chi_{1,\sigma}$. We now have, for all $\sigma \in G_K$,

$$\psi\sigma = \alpha_2^{-1}\alpha_1\sigma = \alpha_2^{-1}g_\sigma\alpha_1\chi(\sigma) = \sigma\alpha_2^{-1}\alpha_1\chi(\sigma) = \sigma\psi\chi(\sigma),$$

which is (10). Note that it follows from this equation that χ is a character. □

of Proposition 24. Let $z \in Z_N''(K)$. Then by Lemma 25 there are elliptic curves E_i/K and level N structures α_i on $E_i \otimes \overline{K}$ for $i = 1, 2$ such that $\mathcal{P}_{\mathcal{Z}_N,\overline{K}}(\langle E_1/\overline{K}, E_2/\overline{K}, \psi\rangle) = z$, where $\psi = \alpha_2^{-1} \circ \alpha_1$. Let χ be the corresponding quadratic character given by Lemma 26. If $E_{2,\chi}/K$ is the twist of E_2/K by χ and $\tau : E_2 \otimes \overline{K} \xrightarrow{\sim} E_{2,\chi} \otimes \overline{K}$ the corresponding isomorphism such that $\tau\chi(\sigma)\sigma = \sigma\tau$, then we have $\langle E_1/\overline{K}, E_{2,\chi}/\overline{K}, \tau\psi\rangle = \langle E_1/\overline{K}, E_2/\overline{K}, \psi\rangle$. By equation (10) we have $\tau\psi\sigma = \tau\chi(\sigma)\sigma\psi = \sigma\tau\psi$, for every $\sigma \in G_K$. Thus, $\tau\psi$ descends to K and so $\langle E_1/K, E_{2,\chi}/K, \tau\psi\rangle \in \mathcal{Z}_N(K)$. We thus have (cf. Remark 23)

$$\begin{aligned}\mathcal{P}_{\mathcal{Z}_N,K}(\langle E_1/K, E_{2,\chi}/K, \tau\psi\rangle) &= \mathcal{P}_{\mathcal{Z}_N,\overline{K}}(\langle E_1/\overline{K}, E_{2,\chi}/\overline{K}, \tau\psi\rangle) \\ &= \mathcal{P}_{\mathcal{Z}_N,\overline{K}}(\langle E_1/\overline{K}, E_2/\overline{K}, \psi\rangle) = z,\end{aligned}$$

which shows that $z \in \mathrm{Im}(\mathcal{P}_{\mathcal{Z}_N,K})$, as claimed. □

For each $\varepsilon \in (\mathbb{Z}/N\mathbb{Z})^\times$, we also have the following subfunctor $\mathcal{Z}_{N,\varepsilon}$ of $\mathcal{Z}_N$ which is defined by

$$\mathcal{Z}_{N,\varepsilon}(S) = \left\{ \langle E_1/S, E_2/S, \psi \rangle \in \mathcal{Z}_N(S) : e_N \circ \psi = e_N^\varepsilon \right\}.$$

It is then clear that $\mathcal{Z}(S) = \coprod \mathcal{Z}_{N,\varepsilon}(S)$.

Restricting the above (functor) morphisms $\mathbf{\Phi}_N$ and $\mathcal{P}_{\mathcal{Y}_N}$ (cf. Remark 21 and Prop. 22) to the component $\mathcal{Y}_{N,\varepsilon}$ of $\mathcal{Y}_N$ yields morphisms

$$\mathbf{\Phi}_{N,\varepsilon} = \mathbf{\Phi}_{N|\mathcal{Y}_{N,\varepsilon}} : \mathcal{Y}_{N,\varepsilon} \to \mathcal{Z}_{N,\varepsilon} \text{ and } \mathcal{P}_{\mathcal{Y}_{N,\varepsilon}} = \mathcal{P}_{\mathcal{Y}_N|\mathcal{Y}_{N,\varepsilon}} : \mathcal{Y}_{N,\varepsilon} \xrightarrow{\sim} h_{Y'_{N,\varepsilon}}.$$

On the other hand, we also have the quotient morphism

$$\Phi_{N,\varepsilon} : Y'_{N,\varepsilon} \to Z'_{N,\varepsilon/\mathbb{Q}} = \tilde{\Delta}_\varepsilon \backslash Y'_{N,\varepsilon}$$

where $Z'_{N,\varepsilon/\mathbb{Q}}$ denotes the non-cuspidal part of the surface $Z_{N,\varepsilon/\mathbb{Q}}$ defined in section 3.2 (cf. Theorem 14 and Remark 15). These morphisms are connected as follows:

Theorem 27. *For every field $K \supset \mathbb{Q}$ there is a* unique *map*

$$\mathcal{P}_{\mathcal{Z}_{N,\varepsilon},K} : \mathcal{Z}_{N,\varepsilon}(K) \to Z'_{N,\varepsilon/\mathbb{Q}}(K)$$

which is compatible with base change (of fields) such that

$$\Phi_{N,\varepsilon} \circ \mathcal{P}_{\mathcal{Y}_{N,\varepsilon},K} = \mathcal{P}_{\mathcal{Z}_{N,\varepsilon},K} \circ \mathbf{\Phi}_{N,\varepsilon}. \tag{11}$$

In addition, $\mathcal{P}_{\mathcal{Z}_{N,\varepsilon},K}$ is a bijection if K is algebraically closed, whereas for an arbitrary field K we have

$$Z''_{N,\varepsilon}(K) \subset \mathrm{Im}(\mathcal{P}_{\mathcal{Z}_{N,\varepsilon},K}).$$

Proof. Define $\mathcal{P}_{\mathcal{Z}_{N,\varepsilon},K} = \mathcal{P}_{\mathcal{Z}_N,K|\mathcal{Z}_{N,\varepsilon}(K)} : \mathcal{Z}_{N,\varepsilon}(K) \to Z'_N(K)$. Then it is clear from Proposition 22 that $\mathcal{P}_{\mathcal{Z}_{N,\varepsilon},K}$ is compatible with base change and that equation (11) holds. In addition, it follows that if K is algebraically closed, then $\mathcal{P}_{\mathcal{Z}_{N,\varepsilon},K}$ is a bijection onto its image. Now by (11), this image has to be $Z_{N,\varepsilon/\mathbb{Q}}(K)$ because it is the image of $\Phi_{N,\varepsilon}$ (and because $\mathbf{\Phi}_{N,\varepsilon,K}$ is surjective). From this we see in particular that for any K, the image of $\mathcal{P}_{\mathcal{Z}_{N,\varepsilon},K}$ is contained in $Z_N(K) \cap Z_{N,\varepsilon/\mathbb{Q}}(\overline{K}) = Z_{N,\varepsilon/\mathbb{Q}}(K)$, and so $\mathcal{P}_{\mathcal{Z}_{N,\varepsilon},K}$ satisfies the requirements of the theorem. $\square$

4.3 Proof of Theorem 2

Lemma 28. *Let* $\langle E_1/\mathbb{Q}, E_2/\mathbb{Q}, \psi\rangle \in \mathcal{Z}_{N,1}(\mathbb{Q})$. *If* E_1 *and* E_2 *are* $\mathbb{Q}$*-isogeneous, then* $\mathcal{P}_{\mathcal{Z}_{N,1},\mathbb{Q}}(\langle E_1, E_2, \psi\rangle_{\mathbb{Q}}) \in M(Z_{N,1})$*, i.e., it is a Mazur trivial point.*

Proof. Since E_1 and E_2 are $\mathbb{Q}$-isogeneous, there is a *cyclic* $\mathbb{Q}$-isogeny between them. If n is its degree, then by the modular description of $X_0'(n)$ we have $\mathcal{P}_{\mathcal{Y}_1,\mathbb{Q}}(\langle E_1, E_2\rangle_{\mathbb{Q}}) \in \xi_n(X_0'(n)(\mathbb{Q}))$, where ξ_n is the normalization map as in section 3.3. By Proposition 22, this implies that $\Psi \circ \mathcal{P}_{Z_{N,1},\mathbb{Q}}(\langle E_1, E_2, \psi\rangle_{\mathbb{Q}}) \in \xi_n(X_0'(n)(\mathbb{Q}))$ and so the assertion follows from the definition of $M(Z_{N,1})$ (cf. section 3.3).

□

of Theorem 2. Consider the infinite number of sections of $\bar{S}_i : \mathbb{P}^1_{\mathbb{Q}} \to \bar{Z}$ given by Theorem 19. By Propositions 4 and 7, the proper transform S_i in $Z/\mathbb{Q}$ of each $\bar{S}_i$ is a curve $S_i \simeq \mathbb{P}^1_{\mathbb{Q}}$ on Z; by construction, $|S_i(\mathbb{Q}) \setminus M| = \infty$, where $M = M(Z_{11,1})$. By Theorem 27 and Lemma 28, the points of $S_i(\mathbb{Q}) \cap Z'(\mathbb{Q}) \setminus M$ correspond to a one-parameter family of isomorphism classes of pairs of elliptic curves over $\mathbb{Q}$ with symplectically isomorphic 11-structure which are not $\mathbb{Q}$-isogeneous, and so we have proved the theorem. □

The authors are very thankful for helpful and stimulating discussions with G. Frey. The second author wants to thank Queen's University and the first author for their hospitality and kindness.

This research was supported in part by a grant from the Natural Science and Engineering Research Council of Canada (NSERC).

References

[1] W. Barth, C. Peters, and A. van de Ven, *Compact Complex Surfaces*, Springer-Verlag, Berlin, 1984.

[2] P. Deligne, *Formes modulaires et représentations ℓ-adiques*, Sem. Bourbaki 1968/69, No. 355. Springer Lecture Notes **179** (1971), 139–172.

[3] P. Deligne and M. Rapoport, *Les schémas de modules de courbes elliptiques*, Modular functions of one variable, II, Lecture Notes in Math. 349, Springer-Verlag, Berlin, 1973, pp. 143–316.

[4] G. Frey and M. Müller, *Arithmetic of modular curves and applications*, Algorithmic Algebra and Number Theory, Heidelberg 1997 (B. H. Matzat, G.-M. Greuel and G. Hiss, eds.), Springer-Verlag, Berlin, 1999, pp. 11–48.

[5] E. Halberstadt and A. Kraus, *On the modular curves* $Y_E(7)$, To appear in Math. Comp.

[6] C. F. Hermann, *Modulflächen quadratischer Diskriminante*, Manuscr. Math. **72** (1991), 95–10.

[7] E. Kani, *On the moduli functor* $\mathcal{Z}_{N,\varepsilon}$, in preparation.

[8] E. Kani and W. Schanz, *Diagonal quotient surfaces*, Manuscr. Math. **93** (1997), 67–108.

[9] E. Kani and W. Schanz, *Modular diagonal quotient surfaces*, Math. Z. **227** (1998), 337–366.

[10] N. M. Katz and B. Mazur, *Arithmetic Moduli of Elliptic Curves*, Princeton University Press, Princeton, NJ, 1985.

[11] M. A. Kenku, *On the number of* $\mathbf{Q}$*-isomorphism classes of elliptic curves in each* $\mathbf{Q}$*-isogeny class*, J. Number Th. **15** (1982), 199–202.

[12] A. Kraus and J. Oesterlé, *Sur une question de B. Mazur*, Math. Ann. **293** (1992), no. 2, 259–275.

[13] S. Lang, *Elliptic Functions*, Addison-Wesley, Reading, MA, 1973.

[14] B. Mazur, *Rational isogenies of prime degree*, Invent. Math. **44** (1978), 129–162.

[15] D. Mumford, *Abelian Varieties*, Oxford University Press, Oxford, 1970.

[16] G. Shimura, *Introduction to the Arithmetic Theory of Automorphic Functions*, Princeton University Press, Princeton, NJ, 1971.

[17] J. H. Silverman, *The Arithmetic of Elliptic Curves*, GTM 106, Springer-Verlag, New York, 1986.

[18] J. H. Silverman, *Advanced Topics in the Arithmetic of Elliptic Curves*, GTM 151, Springer-Verlag, New York, 1994.