Preprint of an article published in International Journal of Mathematics, 29(7): 1850045.
doi:10.1142/S0129167X18500453 © World Scientific Publishing Company
https://doi.org/10.1142/S0129167X18500453

Modular Curves and Symmetries of Hecke Type

Bernhard Heim*, Christian Kaiser† and Atsushi Murase ‡

April 25, 2018

Abstract

We give a characterization of modular curves by a single symmetry of Hecke type. In the proof, we use the theorem of André, which characterizes modular curves in terms of special points.

Keywords: modular curves, symmetries, André-Oort conjecture, Borcherds products.

Mathematics Subject Classification 2010: 11G15, 11G18, 14G35, 14H52, 14K22

1 Introduction and the main results

In [1], André gives a criterion for an irreducible algebraic curve in $\mathbb{C}^2$ to be a modular curve in terms of special points. The aim of the present paper is to give a criterion for an effective divisor in $\mathbb{C}^2$ to be *modular* in terms of a single symmetry of Hecke type.

To be more precise, let $j(E)$ denote the j-invariant of an elliptic curve E. A complex number x is said to be *special* if an elliptic curve E with $j(E) = x$ has complex multiplication. A point (x_1, x_2) in $\mathbb{C}^2$ is said to be *special* if both x_1 and x_2 are special. An isogeny ϕ between elliptic curves is called a *cyclic isogeny* of degree m if $\mathrm{Ker}(\phi)$ is a cyclic group of order m. For a positive integer N, let $Y_0(N) = \Gamma_0(N)\backslash\mathfrak{H}$ be the (open) modular curve of level N classifying cyclic isogenies of degree N between elliptic curves. The map $(\phi\colon E \to E') \mapsto (j(E), j(E'))$ sends $Y_0(N)$ to an irreducible algebraic curve in $\mathbb{C}^2$.

*Department of Mathematics and Science, Faculty of Science, German University of Technology in Oman, Muscat, Sultanate of Oman; Max-Planck-Institute for Mathematics, Vivatsgasse 7, 53111 Bonn, Germany; e-mail: bernhard.heim@gutech.edu.om, heim@mpim-bonn.mpg.de (corresponding author)

†Max-Planck-Institute for Mathematics, Vivatsgasse 7, 53111 Bonn, Germany; e-mail: kaiser@mpim-bonn.mpg.de

‡Faculty of Science, Kyoto Sangyo University, Motoyama, Kamigamo, Kita-ku, 603-8555 Kyoto, Japan; e-mail: murase@cc.kyoto-su.ac.jp

Then the theorem of André ([1]) is stated as follows; see also [6] for another proof assuming Generalized Riemann Hypothesis (GRH).

Theorem 1.1. *Let C be an irreducible algebraic curve in $\mathbb{C}^2$ such that neither of its projections to $\mathbb{C}$ is constant. If C contains infinitely many special points, then C is the image of $Y_0(N)$ in $\mathbb{C}^2$ for some positive integer N.*

This theorem is a special case of the André-Oort conjecture, which says that the irreducible components of the Zariski closure of any set of special points in a Shimura variety are special subvarieties. The conjecture has been proven under GRH in [11] and [9]; for an excellent review of the André-Oort conjecture, see [7].

Our original motivation was to relate Theorem 1.1 to symmetries of Hecke type introduced in [8] (see Remark 1.8). To define symmetries of Hecke type, for a positive integer m, let T_m be the correspondence on $\mathbb{C}$ that sends $j(E)$ to the sum (as a divisor) of $j(E/G)$, where G runs over the cyclic subgroups of E of order m. The graph in $\mathbb{C}^2$ corresponding to T_m is the image of $Y_0(m)$ in $\mathbb{C}^2$ and is given by

$$\left\{ \left(j(\tau), j\left(\frac{a\tau+b}{d}\right)\right) \mid \tau \in \mathfrak{H}, (a,b,d) \in \Lambda(m) \right\},$$

where $j(\tau) := j(\mathbb{C}/(\mathbb{Z}+\tau\mathbb{Z}))$ for $\tau \in \mathfrak{H}$ and

$$\Lambda(m) := \left\{ (a,b,d) \in (\mathbb{Z}_{\geq 0})^3 \mid ad = m, 0 \leq b < d, \gcd(a,b,d) = 1 \right\}.$$

Note that the definition of T_m here is different from the usual one (defined as $j(E) \mapsto$ the sum of $j(E/G)$, where G runs over all subgroups of E of order m) (see [6], page 320). We define the product $X \circ Y$ of correspondences X and Y on $\mathbb{C}$ as in [10], Section 7.2. Recall that

$$T_m \circ T_n = T_{mn} \text{ if } \gcd(m,n) = 1, \tag{1.1}$$

$$T_p \circ T_{p^k} = T_{p^{k+1}} + (p + \delta_{k,1})\, T_{p^{k-1}} \text{ for a prime number } p \text{ and } k \geq 1, \tag{1.2}$$

where $\delta_{k,1}$ is the Kronecker symbol. The correspondences T_m $(m \geq 1)$ generate a commuative subring of the algebra of correspondences on $\mathbb{C}$, which we call the *algebra of Hecke correspondences*.

Let D be an effective divisor in $\mathbb{C}^2$. By definition, $D = \sum_{i=1}^r e_i C_i$ is a formal finite sum of (not necessarily smooth) irreducible algebraic curves C_i in $\mathbb{C}^2$ with $e_i \in \mathbb{Z}_{>0}$. We set

$$T_m^{\uparrow}(D) = (T_m \times 1)D, \quad T_m^{\downarrow}(D) = (1 \times T_m)D.$$

Note that both $T_m^{\uparrow}(D)$ and $T_m^{\downarrow}(D)$ are effective divisors in $\mathbb{C}^2$, and that $T_m^{\uparrow}$ and $T_{m'}^{\downarrow}$ commute with each other for $m, m' \geq 1$. We denote by $\mathrm{supp}(D)$ the union of the irreducible components $C_1, \ldots, C_r$. Often our notation does not distinguish between an effective divisor and its support if the meaning is clear.

Remark 1.2. Let C be an irreducible algebraic curve in $\mathbb{C}^2$ such that neither of its projections to $\mathbb{C}$ is constant. We consider C as a correspondence on $\mathbb{C}$. Then $T_m^{\uparrow}(C)$ (respectively $T_m^{\downarrow}(C)$) is the effective divisor in $\mathbb{C}^2$ corresponding to the product $T_m \circ C$ (respectively $C \circ T_m$).

We give another description of $T_m^{\uparrow}(D)$ and $T_m^{\downarrow}(D)$ when D is the divisor of a polynomial $F \in \mathbb{C}[X, Y]$. It is easily verified that there exist polynomials $\mathcal{T}_m^{\uparrow}(F)$ and $\mathcal{T}_m^{\downarrow}(F)$ in $\mathbb{C}[X, Y]$ satisfying

$$\mathcal{T}_m^{\uparrow}(F)\left(j(\tau), j(\tau')\right) = \prod_{(a,b,d)\in\Lambda(m)} F\left(j\left(\frac{a\tau + b}{d}\right), j(\tau')\right),$$

$$\mathcal{T}_m^{\downarrow}(F)\left(j(\tau), j(\tau')\right) = \prod_{(a,b,d)\in\Lambda(m)} F\left(j(\tau), j\left(\frac{a\tau' + b}{d}\right)\right)$$

for $\tau, \tau' \in \mathfrak{H}$. Then $T_m^{\uparrow}(D)$ and $T_m^{\downarrow}(D)$ are the divisors of $\mathcal{T}_m^{\uparrow}(F)$ and $\mathcal{T}_m^{\downarrow}(F)$ respectively.

Define $\Phi_1(X, Y) := X - Y$ and $\Phi_m(X, Y) := \mathcal{T}_m^{\downarrow}(\Phi_1)(X, Y)$ for $m \geq 2$. Note that $\mathcal{T}_m^{\uparrow}(\Phi_1)(X, Y) = \pm\Phi_m(X, Y)$. We see that $\Phi_m(X, Y)$ is the modular polynomial of order m (for example, see Section 11.B in [5]).

We say that an effective divisor $D = \sum_{i=1}^{r} e_i C_i$ in $\mathbb{C}^2$ is *modular* if every irreducible component C_i $(i = 1, \ldots, r)$ is the graph of T_{m_i} for some positive integer m_i. The next result follows immediately from Remark 1.2 and the commutativity of the algebra of Hecke correspondences.

Lemma 1.3. *Let D be a modular divisor in $\mathbb{C}^2$. Then*

$$T_m^{\uparrow}(D) = T_m^{\downarrow}(D) \tag{1.3}$$

holds for every $m \geq 1$.

One of the results of [8] essentially shows that the converse of Lemma 1.3 holds for effective divisors.

Theorem 1.4 ([8],Theorem 8.1). *Let D be an effective divisor in $\mathbb{C}^2$ and suppose that (1.3) holds for any $m \geq 1$. Then D is modular.*

Remark 1.5. Theorem 8.1 in [8] is stated as a characterization of modular equations (or holomorphic Borcherds products on $O(2, 2)$) by symmetries. The proof in [8] is analytic and uses the theory of Borcherds products on $O(2, 2)$. We also note that a characterization of holomorphic Borcherds products on $O(2, n)$ $(n \geq 2)$ by symmetries of Hecke type is given in [8] (for Borcherds products, see [2], [3] and [4]). It would be interesting to study relations between symmetries for automorphic forms on $O(2,n)$ and the André-Oort conjecture for Shimura varieties attached to $O(2,n)$.

The aim of the present paper is to show the following improved version of Theorem 1.4 saying that only one single symmetry is needed for D to be modular.

Theorem 1.6. *Let D be an effective divisor in $\mathbb{C}^2$ and assume that $T_p^{\uparrow}(D) = T_p^{\downarrow}(D)$ holds for some prime number p. Then D is modular.*

As a direct consequence of Theorem 1.6, we have the following result:

Corollary 1.7. *Let $F(X,Y)$ be a nonzero polynomial in $\mathbb{C}[X,Y]$ such that $\mathcal{T}_p^{\uparrow}(F)$ is a constant multiple of $\mathcal{T}_p^{\downarrow}(F)$ for some prime number p. Then*

$$F(X,Y) = c\prod_{i=1}^{r}\Phi_{N_i}(X,Y)^{e_i},$$

where $c \in \mathbb{C}^{\times}$, N_i's are distinct positive integers and $e_i \in \mathbb{Z}_{>0}$ $(i = 1, \ldots, r)$.

The proof of Theorem 1.6 is algebro-geometric and is an application of the theorem of André.

Remark 1.8. Let C be an irreducible algebraic curve in $\mathbb{C}^2$. The symmetry $T_m^{\uparrow}(C) = T_m^{\downarrow}(C)$ implies the inclusion

$$C \subset (T_m \times T_m)C, \tag{1.4}$$

since

$$(T_m \times T_m)C = (T_m \times 1)(1 \times T_m)C = (T_m \times 1)(T_m \times 1)C = ((T_m \circ T_m) \times 1)C$$

and $T_m \circ T_m = \sum_{k\geq 1} a_k T_k$ (a finite sum) with $a_k \in \mathbb{Z}_{\geq 0}$ and $a_1 > 0$. Edixhoven showed without GRH ([6], Theorem 6.1) that C is modular if (1.5) holds for a sufficiently large square free integer m. It is unclear to the authors whether Edixhoven's proof can be modified to work for effective divisors respectively without the assumption on m. The generality of effective divisors is important for applying the theorem to divisors of holomorphic automorphic forms on $O(2,2)$ to get a characterization of holomorphic Borcherds products or modular equations (Corollary 1.7).

2 The proof of Theorem 1.6

Throughout this section, we let $D = \sum_{i=1}^{r} e_i C_i$ be an effective divisor in $\mathbb{C}^2$ and assume that $T_p^{\uparrow}(D) = T_p^{\downarrow}(D)$ holds for some prime number p. The equality (1.2) implies that there exists a polynomial $G_n(t)$ of degree n such that $T^{\uparrow}_{p^n} = G_n(T^{\uparrow}_p)$ and $T^{\downarrow}_{p^n} = G_n(T^{\downarrow}_p)$. It follows that

$$T^{\uparrow}_{p^n}(D) = T^{\downarrow}_{p^n}(D) \tag{2.1}$$

holds for any $n \geq 1$.

Lemma 2.1. *The divisor D has no irreducible component of the type $\{x_0\} \times \mathbb{C}$ or $\mathbb{C} \times \{y_0\}$ with $x_0, y_0 \in \mathbb{C}$.*

Proof. Let $C_0 = \{x_0\} \times \mathbb{C}$ with $x_0 \in \mathbb{C}$. Take $\tau_0 \in \mathfrak{H}$ such that $j(\tau_0) = x_0$. Then

$$T^{\uparrow}_{p^n}(C_0) = \sum_{(a,b,d)\in\Lambda(p^n)} (\{x_{a,b,d}\} \times \mathbb{C}) \quad \text{and} \quad T^{\downarrow}_{p^n}(C_0) = (p^n + p^{n-1})C_0,$$

where $x_{a,b,d} = j\left(\dfrac{a\tau_0 + b}{d}\right) \in \mathbb{C}$. Since the number of distinct points in $\{x_{a,b,d}\}_{(a,b,d)\in\Lambda(p^n)}$ goes to infinity as $n \to \infty$, D has no component of the type C_0. In a similar way, we can show that D has no component of the type $\mathbb{C} \times \{y_0\}$, which proves the lemma. □

Let E, E' be elliptic curves and m a positive integer. We write $E \overset{m\text{-cyclic}}{\longrightarrow} E'$ if there exists a cyclic isogeny $\phi\colon E \to E'$ of degree m. Observe that, for an irreducible algebraic curve C,

$$T^{\uparrow}_m(C) = \left\{(x,y) \in \mathbb{C}^2 \mid \text{there exists } x' \in \mathbb{C} \text{ with } (x',y) \in C \text{ and } E_x \overset{m\text{-cyclic}}{\longrightarrow} E_{x'}\right\},$$
$$T^{\downarrow}_m(C) = \left\{(x,y) \in \mathbb{C}^2 \mid \text{there exists } y' \in \mathbb{C} \text{ with } (x,y') \in C \text{ and } E_y \overset{m\text{-cyclic}}{\longrightarrow} E_{y'}\right\}.$$

Here, for $x \in \mathbb{C}$, we choose and fix an elliptic curve E_x with $j(E_x) = x$.

We say that an elliptic curve E satisfies the condition (A) if there exist endomorphisms ϕ_j of E with $\mathrm{Ker}(\phi_j) \simeq \mathbb{Z}/p^{m_j}\mathbb{Z}$, where $m_1 < m_2 < \cdots$ is an infinite increasing sequence of positive integers. Note that $x \in \mathbb{C}$ is special if E_x satisfies (A).

Lemma 2.2. *There exist infinitely many $x \in \mathbb{C}$ such that E_x satisfies (A).*

Proof. There exist infinitely many imaginary quadratic fields K_j such that p splits in the integer ring L_j of K_j: $p = \mathfrak{p}_j\overline{\mathfrak{p}_j}$. Let $\mathfrak{p}_j^{h_j} = \pi_j L_j$, where $\pi_j \in L_j$ and h_j is the class number of K_j. The elliptic curve $\mathbb{C}/L_j$ has cyclic endomorphisms of degree $p^{h_j m}$ given by $z \mapsto \pi_j^m z$ for $m \geq 1$, which implies that $\mathbb{C}/L_j$ satisfies (A). This completes the proof of the lemma. □

Proposition 2.3. *Let $(x,y) \in \mathbb{C}^2$ be a closed point of $\mathrm{supp}(D)$. If E_x satisfies (A), then E_y also satisfies (A).*

Proof. Let $(x, y) \in \mathrm{supp}(D)$ and suppose that E_x satisfies (A). Then there exists an infinite increasing sequence $m_1 < m_2 < \cdots$ with $E_x \overset{p^{m_j}\text{-cyclic}}{\longrightarrow} E_x$. We thus have $(x, y) \in T^{\uparrow}_{p^{m_j}}(D) = T^{\downarrow}_{p^{m_j}}(D)$ by the symmetries (2.1). This implies that there exist $y_1, y_2, \ldots \in \mathbb{C}$ with $(x, y_i) \in \mathrm{supp}(D)$ and $E_y \overset{p^{m_j}\text{-cyclic}}{\longrightarrow} E_{y_j}$. In view of Lemma 2.1, taking a suitable subsequence of $\{y_j\}$, we may (and do) assume that $y_1 = y_2 = \cdots$, for which we write y'. Then there exists a cyclic isogeny $\phi_j \colon E_y \to E_{y'}$ of degree p^{m_j} for any $j \geq 1$. Define $\varphi_j := \phi_1^* \circ \phi_j \in \mathrm{End}(E_y)$, where ϕ_1^* denotes the dual of ϕ_1. Note that ϕ_1^* is also a cyclic isogeny of E_y of degree p^{m_1}. We decompose φ_j into the composition of the multiplication-by-p^{k_j} endomorphism of E_y and a cyclic endomorphism ψ_j of E_y of degree p^{l_j}. Since $\mathrm{Ker}(\varphi_j)$ is an extension of $\mathbb{Z}/p^{m_1}\mathbb{Z}$ by $\mathbb{Z}/p^{m_j}\mathbb{Z}$, we have $\mathrm{Ker}(\varphi_j) \cong \mathbb{Z}/p^{\kappa_j}\mathbb{Z} \times \mathbb{Z}/p^{\mu_j}\mathbb{Z}$ with $\kappa_j \leq \min(m_1, m_j) = m_1$ and $\mu_j \geq \max(m_1, m_j) = m_j$. Thus we have $k_j = \kappa_j \leq m_1$ for $j \geq 1$. This implies that $\lim_{j\to\infty} l_j = \infty$, which shows that E_y satisfies (A). $\square$

We now prove Theorem 1.6. By Lemma 2.1, neither of the two projections of C_i to $\mathbb{C}$ is constant for every i. By Lemma 2.2, there exist infinitely many closed points (x_n, y_n) of $\mathrm{supp}(D)$ such that E_{x_n} satisfies (A). Then E_{y_n} also satisfies (A) by Proposition 2.3. It follows that the points (x_n, y_n) are special and hence that, for some i, C_i contains infinitely many special points. By the theorem of André (Theorem 1.1), C_i is the image of $Y_0(N)$ for some positive integer N. Since $D' = D - e_i C_i$ also satisfies the symmetry $T^{\uparrow}_p(D') = T^{\downarrow}_p(D')$ by Lemma 1.3, the proof of the theorem is completed by induction on r.

Acknowledgement

The first author thanks the Max Planck Institute for Mathematics for support and an invitation in July and August 2017. He also thanks Prof. Krieg for useful discussions at the Graduate school: Experimental and constructive algebra, at the RWTH Aachen. The third author is partially supported by Grants-in-Aids from JSPS (17K05186). The authors are grateful to the referee for the valuable comments and suggestions.

References

[1] Y. André, Finitude des couples d'invariants modulaires singuliers sur une courbe algébrique plane non modulaire, *J. Reine Angew. Math.* **505** (1998), 203–208.

[2] R. E. Borcherds, Automorphic forms on $O_{s+2,2}(\mathbb{R})$ and infinite products, *Invent. Math.* **120** (1995), 161–213.

[3] R. E. Borcherds, Automorphic forms with singularities on Grassmannians, *Invent. Math.* **132** (1998), 491–562.

[4] J. H. Bruinier, *Borcherds Products on $O(2, l)$ and Chern Classes of Heegner Divisors*, Lecture Notes in Math. **1780**, Springer Verlag, Berlin, 2002.

[5] D. A. Cox, *Primes of the form $x^2 + ny^2$. Fermat, class field theory and complex multiplication*, A Wiley-Interscience Publication, New York, 1989.

[6] S. J. Edixhoven, Special points on the product of two modular curves, *Compositio Math.* **114** (1998), 315–328.

[7] S. J. Edixhoven and L. Taelman, The André-Oort conjecture, *Nieuw Arch. Wiskd.* **15** (2014), 279–282.

[8] B. Heim and A. Murase, A characterization of holomorphic Borcherds lifts by symmetries, *Int. Math. Res. Not.* **21** (2015), 11150-11185. (DOI: 10.1093/imrn/rnv021).

[9] B. Klinger and A. Yafaev, The André-Oort conjecture, *Ann. of Math.* **180** (2014), 867–925.

[10] G. Shimura, *Introduction to the Arithmetic Theory of Automorphic Functions*, Iwanami Shoten and Princeton University Press, 1971.

[11] E. Ullmo and A. Yafaev, Galois orbits and equidistribution of special subvarieties: towards the André-Oort conjecture, *Ann. of Math.* **180** (2014), 823–865.