Modular parametrizations of certain elliptic curves

Matija Kazalicki, Yuichi Sakai and Koji Tasaka

Abstract

Kaneko and Sakai [11] recently observed that certain elliptic curves whose associated newforms (by the modularity theorem) are given by the eta-quotients can be characterized by a particular differential equation involving modular forms and Ramanujan-Serre differential operator.

In this paper, we study certain properties of modular parametrization associated to the elliptic curves over $\mathbb{Q}$, and as a consequence we generalize and explain some of their findings.

1. Introduction

By the modularity theorem [4, 8], an elliptic curve E over $\mathbb{Q}$ admits a modular parametrization $\Phi_E : X_0(N) \to E$ for some integer N. If N is the smallest such integer, then it is equal to the conductor of E and the pullback of the Néron differential of E under Φ_E is a rational multiple of $2\pi i f_E(\tau)$, where $f_E(\tau) \in S_2(\Gamma_0(N))$ is a newform with rational Fourier coefficients. The fact that the L-function of $f_E(\tau)$ coincides with the Hasse-Weil zeta function of E (which follows from Eichler-Shimura theory) is central to the proof of Fermat's last theorem, and is related to the Birch and Swinnerton-Dyer conjecture. In addition to this, modular parametrization is used for constructing rational points on elliptic curves, and appears in the Gross-Zagier formula [9].

In this paper, we study some general properties of Φ_E, and as a consequences we explain and generalize the results of Kaneko and Sakai from [11].

Kaneko and Sakai (inspired by the paper of Guerzhoy [10]) observed that certain elliptic curves whose associated newforms (by the modularity theorem) are given by the eta-quotients from the list of Martin and Ono [12] can be characterized by a particular differential equation involving holomorphic modular forms.

To give an example of this phenomena, let $f_{20}(\tau) = \eta(\tau)^4\eta(5\tau)^4$ be a unique newform of weight 2 on $\Gamma_0(20)$, where $\eta(\tau)$ is the Dedekind eta function $\eta(\tau) = q^{1/24}\prod_{n>0}(1-q^n)$, $q = e^{2\pi i\tau}$, and put $\Delta_{5,4}(\tau) = f_{20}(\tau/2)^2$. Then an Eisenstein series $Q_5(\tau)$ on $M_4(\Gamma_0(5))$ associated either to cusp $i\infty$ or to cusp 0 is a solution of the following differential equation

$$\partial_{5,4}(Q_5)^2 = Q_5^3 - \frac{89}{13}Q_5^2\Delta_{5,4} - \frac{3500}{169}Q_5\Delta_{5,4}^2 - \frac{125000}{2197}\Delta_{5,4}^3, \tag{1}$$

where $\partial_{5,4}(Q_5(\tau)) = \frac{1}{2\pi i}Q_5(\tau)' - \frac{1}{2\pi i}Q_5(\tau)\Delta_{5,4}(\tau)'/\Delta_{5,4}(\tau)$ is a Ramanujan-Serre differential operator. Throughout the paper, we use symbol $'$ to denote $\frac{d}{d\tau}$. This differential equation defines

2010 Mathematics Subject Classification 11G05 (primary), 11F11, 11F30 (secondary)
Keywords: modular parametrization, modular forms, Ramanujan-Serre differential operator, modular degree

a parametrization of an elliptic curve $E : y^2 = x^3 - \frac{89}{13}x^2 - \frac{3500}{169}x - \frac{125000}{2197}$ by modular functions

$$x = \frac{Q_5(\tau)}{\Delta_{5,4}(\tau)}, \quad y = \frac{\partial_{5,4}(Q_5)(\tau)}{\Delta_{5,4}(\tau)^{3/2}},$$

and $f_{20}(\tau)$ is the newform associated to E. One finds that $\Delta_{5,4}(\tau) \in S_4(\Gamma_0(5))$, so curiously the modular forms $\Delta_{5,4}, Q_5$ and $\partial(Q_5)$ appearing in this parametrization are modular for $\Gamma_0(5)$, although the conductor of E is 20.

Using the Eichler-Shimura theory, we generalize (1) to the arbitrary elliptic curve E of conductor $4N$, $E : y^2 = x^3 + ax^2 + bx + c$, where $a, b, c \in \mathbb{Q}$, which admits a modular parametrization $\Phi : X \to E$ satisfying

$$\Phi^*\left(\frac{dx}{2y}\right) = \pi i f_{4N}(\tau/2)d\tau.$$

Here X is the modular curve $\mathbb{H}/\left(\begin{smallmatrix} \frac{1}{2} & 0 \\ 0 & 1 \end{smallmatrix}\right)^{-1}\Gamma_0(4N)\left(\begin{smallmatrix} \frac{1}{2} & 0 \\ 0 & 1 \end{smallmatrix}\right)$, and $f_{4N}(\tau) \in S_2(\Gamma_0(4N))$ is a newform with rational Fourier coefficients associated to E. It follows from the modularity theorem that in any $\mathbb{Q}$-isomorphism class of elliptic curves there is an elliptic curve E admitting such parametrization (note that for $u \in \mathbb{Q}^\times$ the change of variables $x = u^2X$ and $y = u^3Y$ implies $\frac{dX}{Y} = u\frac{dx}{y}$).

To such Φ we associate a solution $Q(\tau) = x(\Phi(\tau))f_{4N}(\tau/2)^2$ of a differential equation

$$\partial_{N,4}(Q)^2 = Q^3 + aQ^2\Delta_{N,4} + bQ\Delta_{N,4}^2 + c\Delta_{N,4}^3, \tag{2}$$

where $\Delta_{N,4}(\tau) = f_{4N}(\tau/2)^2$, and $\partial_{N,4}(Q(\tau)) = \frac{1}{2\pi i}Q(\tau)' - \frac{1}{2\pi i}Q(\tau)\Delta_{N,4}(\tau)'/\Delta_{N,4}(\tau)$.

We show in Corollary 12 that $f_{4N}(\tau/2)^2$ is modular for $\Gamma_0(N)$. In general the solution $Q(\tau)$ will not be holomorphic and will be modular only for $\left(\begin{smallmatrix} \frac{1}{2} & 0 \\ 0 & 1 \end{smallmatrix}\right)^{-1}\Gamma_0(4N)\left(\begin{smallmatrix} \frac{1}{2} & 0 \\ 0 & 1 \end{smallmatrix}\right)$, but if the preimage of the point at infinity of E under Φ is contained in cusps of X and is invariant under the action of $\left(\begin{smallmatrix} 1 & 0 \\ N & 1 \end{smallmatrix}\right)$ and $\left(\begin{smallmatrix} 1 & 1 \\ 0 & 1 \end{smallmatrix}\right)$ (acting on X by Möbius transformations), $Q(\tau)$ will be both holomorphic and modular for $\Gamma_0(N)$ (for more details see Proposition 5 and Theorem 7). Moreover, in Theorem 6 we show that there are only finitely many (up to isomorphism) elliptic curves E admitting Φ with these two properties.

We also obtain similar results generalizing the other examples from [11] that correspond to the elliptic curves over $\mathbb{Q}$ with j-invariant 0 and 1728 (see the next section).

2. Main results

Throughout the paper, let N be a positive integer and $k \in \{4, 6, 8, 12\}$. Let $E_k/\mathbb{Q}$ be an elliptic curve given by the short Weierstrass equation $y^2 = f_k(x)$, where

$$\begin{aligned} f_4(x) &= x^3 + a_2x^2 + a_4x + a_6, \\ f_6(x) &= x^3 + b_6, \\ f_8(x) &= x^3 + c_4x, \\ f_{12}(x) &= x^3 + d_6, \end{aligned}$$

and $a_2, a_4, a_6, b_6, c_4, d_6 \in \mathbb{Q}$. Moreover, we assume $j(E_4) \neq 0, 1728$.

Let

$$f_{N,k}(\tau) \in S_2\left(\Gamma_0\left(\frac{k^2}{4}N\right)\right)$$

be a newform with rational Fourier coefficients, and let $\Gamma_k := \begin{pmatrix} \frac{2}{k} & 0 \\ 0 & 1 \end{pmatrix}^{-1} \Gamma_0(\frac{k^2}{4}N) \begin{pmatrix} \frac{2}{k} & 0 \\ 0 & 1 \end{pmatrix}$. Define

$$\Delta_{N,k}(\tau) := f_{N,k}(2\tau/k)^{k/2} \in S_k(\Gamma_k).$$

For $f(\tau) \in M_4^{\mathrm{mer}}(\Gamma_k)$, we define the (Ramanujan-Serre) differential operator by

$$\partial_{N,k}(f(\tau)) = \frac{k}{8\pi i} f'(\tau) - \frac{1}{2\pi i} f(\tau) \frac{\Delta'_{N,k}(\tau)}{\Delta_{N,k}(\tau)} \in M_6^{\mathrm{mer}}(\Gamma_k).$$

Finally, assume that there is a meromorphic modular form $Q_k(\tau) \in M_4^{\mathrm{mer}}(\Gamma_k)$, such that the corresponding differential equation holds

$$\begin{array}{rcl} \partial_{N,4}(Q_4(\tau))^2 &=& Q_4(\tau)^3 + a_2 Q_4(\tau)^2 \Delta_{N,4}(\tau) + a_4 Q_4(\tau) \Delta_{N,4}(\tau)^2 + a_6 \Delta_{N,4}(\tau)^3 \\ \partial_{N,6}(Q_6(\tau))^2 &=& Q_6(\tau)^3 + b_6 \Delta_{N,6}(\tau)^2 \\ \partial_{N,8}(Q_8(\tau))^2 &=& Q_8(\tau)^3 + c_4 Q_8(\tau) \Delta_{N,8}(\tau) \\ \partial_{N,12}(Q_{12}(\tau))^2 &=& Q_{12}(\tau)^3 + d_6 \Delta_{N,12}(\tau). \end{array} \tag{3}$$

Each of these four identities defines a modular parametrization $\Psi_k : X_k \to E_k$

$$\Psi_k(\tau) = \left(\frac{Q_k(\tau)}{\Delta_{N,k}(\tau)^{4/k}}, \frac{\partial_{N,k}(Q_k)(\tau)}{\Delta_{N,k}(\tau)^{6/k}} \right),$$

where X_k is the compactified modular curve $\mathbb{H}/\Gamma_k$.

Proposition 1. *Let $\frac{dx}{2y}$ be the Néron differential on E_k. Then*

$$\Psi_k^* \left(\frac{dx}{2y} \right) = \frac{4\pi i}{k} f_{N,k}(2\tau/k) d\tau. \tag{4}$$

In particular, the conductor of E_k is $\frac{k^2}{4}N$ and $f_{N,k}(\tau)$ is the cusp form associated to E_k by the modularity theorem.

Remark 2. *Note that when $k = 6, 8$ or 12, $f_{N,k}(\tau)$ is a modular form with complex multiplication by the ring of integers of $\mathbb{Q}(\sqrt{-3})$, $\mathbb{Q}(\sqrt{-1})$ and $\mathbb{Q}(\sqrt{-3})$ respectively.*

Conversely, given a modular parametrization $\Phi_k : X_k \to E_k$ satisfying (4), we construct a differential equation (3) and its solution $Q_k(\tau)$ as follows.

Let x and y be functions on E_k satisfying Weierstrass equation $y^2 = f_k(x)$. Functions $x(\tau) := x \circ \Phi_k(\tau)$ and $y(\tau) := y \circ \Phi_k(\tau)$ satisfy $y(\tau)^2 = f_k(x(\tau))$. Moreover (4) implies that

$$\left(\frac{k}{8\pi i} x'(\tau) \right)^2 = f_{N,k}(2\tau/k)^2 y(\tau)^2 = \Delta_{N,k}(\tau)^{4/k} f_k(x(\tau)). \tag{5}$$

Define $Q_k(\tau) := x(\tau) \Delta_{N,k}(\tau)^{4/k}$.

Proposition 3. *The following formula holds*

$$\partial_{N,k}(Q_k(\tau))^2 = \Delta_{N,k}(\tau)^{12/k} f_k(x(\tau)).$$

In particular, $Q_k(\tau)$ is a solution of (3).

Now we investigate conditions under which $Q_k(\tau)$ is holomorphic. The following lemma easily follows from the formula above.

Lemma 4. *Assume that $\tau_0 \in X_k$ is a pole of $x(\tau)$. Then*

$$ord_{\tau_0}(Q_k(\tau)) = \begin{cases} 0, & \text{if } \tau_0 \text{ is a cusp,} \\ -2, & \text{if } \tau_0 \in \mathbb{H}. \end{cases}$$

As a consequence, we have the following characterization of the holomorphicity of $Q_k(\tau)$ in terms of modular parametrization Φ_k. Denote by $\mathcal{C}$ the set of cusps of X_k, and by $\mathcal{O}$ the point at infinity of E_k.

Proposition 5. *We have that $Q_k(\tau)$ is holomorphic if and only if $\Phi_k^{-1}(\mathcal{O}) \subset \mathcal{C}$.*

In Section 3.2 we show that the degree of Φ_k (as a function of the conductor) grows faster than the total ramification index at cusps hence the following theorem holds.

Theorem 6. *There are finitely many elliptic curves $E/\mathbb{Q}$ (up to a $\mathbb{Q}$-isomorphism) that admit a modular parametrization $\Phi : X_k \to E$ with the property that $\Phi^{-1}(\mathcal{O}) \subset \mathcal{C}$.*

In particular, there are finitely many elliptic curves E_k (up to a $\mathbb{Q}$-isomorphism) for which $Q_k(\tau)$ (which satisfy equation (3)) is holomorphic.

Define $A = \left(\begin{smallmatrix} 1 & 0 \\ N & 1 \end{smallmatrix}\right)$ and $T = \left(\begin{smallmatrix} 1 & 1 \\ 0 & 1 \end{smallmatrix}\right)$. It is easy to see that Γ_k is generated by $\Gamma_0(N)$ and A and T (Lemma 9), hence $Q_k(\tau)$ is modular for $\Gamma_0(N)$ if and only if it is invariant under the action of slash operators $|A$ and $|T$. The following theorem describes the modularity in terms of parametrization Φ_k.

Theorem 7. *If $\Phi_k^{-1}(\mathcal{O})$ is invariant under A and T, then $Q_k(\tau)$ is modular for $\Gamma_0(N)$.*

3. Proofs

3.1 Proof of Proposition 1 and Proposition 3

Proof of Proposition 1.

$$\begin{aligned} \Psi_k^*\left(\frac{dx}{2y}\right) &= \frac{1}{2}\frac{d}{d\tau}\left(\frac{Q_k(\tau)}{\Delta_{N,k}(\tau)^{4/k}}\right)\frac{\Delta_{N,k}(\tau)^{6/k}}{\partial_{N,k}(Q_k)(\tau)}d\tau \\ &= \frac{1}{2}\frac{\frac{d}{d\tau}Q_k(\tau)f_{N,k}(2\tau/k)^2 - \frac{d}{d\tau}f_{N,k}(2\tau/k)^2Q_k(\tau)}{f_{N,k}(2\tau/k)^4}\frac{f_{N,k}(2\tau/k)^3}{\frac{k}{8\pi i}\frac{d}{d\tau}Q_k(\tau) - Q_ks(\tau)\frac{\frac{d}{d\tau}f_{N,k}(2\tau/k)^{k/2}}{2\pi i f_{N,k}(2\tau/k)^{k/2}}}d\tau \\ &= \frac{4\pi i}{k}f_{N,k}(2\tau/k)d\tau. \end{aligned}$$

□

Proof of Proposition 3. By definition,

$$\begin{aligned} \partial_{N,k}(Q_k(\tau)) &= \frac{k}{8\pi i}(x(\tau)\Delta_{N,k}(\tau)^{4/k})' - \frac{1}{2\pi i}x(\tau)\Delta_{N,k}(\tau)^{4/k}\frac{\Delta'_{N,k}(\tau)}{\Delta_{N,k}(\tau)} \\ &= \frac{k}{8\pi i}x'(\tau)\Delta_{N,k}(\tau)^{4/k}. \end{aligned}$$

Hence the claim follows from (5). □

3.2 Proof of Theorem 6

Let $e_x \in \mathbb{Z}$ be the ramification index of Φ_k at $x \in X_k$, and let $\deg(\Phi_k)$ be the degree of Φ_k. It follows from the Hurwitz formula that $\sum_{x \in X_k}(e_x - 1) = 2g - 2$, where g is the genus of X_k (note that the genus of X_k is equal to the genus of $\Gamma_0(\frac{k^2}{4}N)$). Therefore $\Phi_k^{-1}(\mathcal{O}) \subset \mathcal{C}$ implies

$$\deg(\Phi_k) \leqslant \sum_{x \in \mathcal{C}} e_x \leqslant 2g - 2 + \#\mathcal{C}. \tag{6}$$

In [15], Watkins proved a lower bound for the degree of modular parametrization Φ of an elliptic curve over $\mathbb{Q}$ of conductor M

$$\deg(\Phi) \geqslant \frac{M^{7/6}}{\log M} \cdot \frac{1/10300}{\sqrt{0.02 + \log\log M}}.$$

On the other hand, an upper bound (see [6]) for the genus g of $X_0(M)$ is

$$g < M \frac{e^\gamma}{2\pi^2}(\log\log M + 2/\log\log M) \text{ for } M > 2,$$

where $\gamma = 0.5772\ldots$ is Euler's constant.

If we use a trivial bound $\#\mathcal{C} \leqslant M$, an easy calculation shows that (6) can not hold for curves E_k of conductor greater than 10^{50}. Therefore, we have proved the Theorem 6.

Remark 8. *If we assume that ramification index at cusps is bounded by 24 (as suggested in the paper of Brunault [5]), and if we use Abramovich [1] lower bound for modular degree* $\deg(\Phi) \geqslant 7M/1600$, *we obtain that (6) can not hold for elliptic curves of conductor greater than* 2^{19}.

3.3 Proof of Theorem 7

In this section we investigate conditions on modular parametrization Φ_k under which $\Delta_{N,k}(\tau)$ and $Q_k(\tau)$, initially modular for Γ_k, are modular for $\Gamma_0(N)$.

For $S = \left(\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right) \in \mathrm{SL}_2(\mathbb{Z})$, and a (meromorphic) modular form $f(\tau)$ of weight l, we define the usual slash operator as $f(\tau)|_l S := f(S\tau)(c\tau + d)^{-l}$, where $S\tau = \frac{a\tau+b}{c\tau+d}$. Define $T = \left(\begin{smallmatrix} 1 & 1 \\ 0 & 1 \end{smallmatrix}\right)$ and $A = \left(\begin{smallmatrix} 1 & 0 \\ N & 1 \end{smallmatrix}\right)$.

Lemma 9. *Group* $\Gamma_0(\frac{k}{2}N)$ *is generated by* Γ_k *and* T, *while* $\Gamma_0(N)$ *is generated by* $\Gamma_0(\frac{k}{2}N)$ *and* A.

Proof. To prove the first statement, let $\left(\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right) \in \Gamma_0(\frac{k}{2}N)$. Then $\gcd(a, \frac{k}{2}) = 1$, and there is $r \in \mathbb{Z}$ such that $ar \equiv -b \bmod \frac{k}{2}$. Then $\left(\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right)T^r \in \Gamma_k = \Gamma_0(\frac{k}{2}N) \cap \Gamma^0(\frac{k}{2})$, and the claim follows.

Second statement is proved analogously. $\square$

Therefore, to prove that $\Delta_{N,k}(\tau)$ and $Q_k(\tau)$ are modular for $\Gamma_0(N)$ it suffices to show their invariance under the slash operators $|T$ and $|A$.

Lemma 10. *Matrices* A *and* T *normalize* Γ_k.

Proof. Let $\left(\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right) \in \Gamma_k = \Gamma_0(\frac{k}{2}N) \cap \Gamma^0(\frac{k}{2})$. Then $\frac{k}{2}N|c$ and $\frac{k}{2}|c$, and $ad \equiv 1 \pmod{\frac{k}{2}}$. In particular, since $\frac{k}{2} \in \{2, 3, 4, 6\}$, it follows that $a \equiv d \pmod{\frac{k}{2}}$.

Since

$$\begin{aligned} A^{-1}\left(\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right)A &= \left(\begin{smallmatrix} a+bN & b \\ -aN-bN^2+c+dN & -bN+d \end{smallmatrix}\right), \\ T^{-1}\left(\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right)T &= \left(\begin{smallmatrix} a-c & a+b-c-d \\ c & c+d \end{smallmatrix}\right), \end{aligned}$$

the claim follows. $\square$

For a prime p, define the Hecke operator T_p as a double coset operator $\Gamma_k\left(\begin{smallmatrix} 1 & 0 \\ 0 & p \end{smallmatrix}\right)\Gamma_k$ acting on the space of cusp forms on Γ_k. Slash operators $|A$ and $|T$ correspond to $\Gamma_k A \Gamma_k$ and $\Gamma_k T \Gamma_k$ (see Chapter 5 of [8]).

Define the Fricke involution $|_2 B$ on $S_2(\Gamma_k)$ by the matrix $B := \begin{pmatrix} 0 & -\frac{k}{2} \\ \frac{k}{2}N & 0 \end{pmatrix}$. Note that $|_2 B$ is the conjugate of the usual Fricke involution on $\Gamma_0(\frac{k^2}{4}N)$. In particular, B normalizes Γ_k, and $|_2 B$ commutes with all the Hecke operators T_p, $p \nmid \frac{k^2}{4}N$. Hence, $f_{N,k}(2\tau/k)|_2 B = \lambda_{k,N} f_{N,k}(2\tau/k)$ for some $\lambda_{k,N} = \pm 1$.

Lemma 11. *The following are true.*

a)

$$f_{N,k}(2\tau/k)|_2 T = e^{4\pi i/k} f_{N,k}(2\tau/k),$$

b)

$$f_{N,k}(2\tau/k)|_2 A = e^{-4\pi i/k} f_{N,k}(2\tau/k).$$

In particular, $|_2 A$ *and* $|_2 B$ *have order* $\frac{k}{2}$ *when acting on* $f_{N,k}(2\tau/k)$.

Proof. A key observation is that the Fourier coefficients of $f_{N,k}(\tau)$ are supported at integers that are 1 mod $\frac{k}{2}$. This implies

$$f_{N,k}(2\tau/k)|_2 T = e^{4\pi i/k} f_{N,k}(2\tau/k).$$

When $k = 4$ (and $k = 12$) this is a consequence of the general fact that $a_f(2) = 0$ whenever $f(\tau) = \sum a_f(n) q^n$ is a newform of level divisible by 4 (see [13], p.29). In the other three cases, $f_{N,k}(\tau)$ is a modular form with complex multiplication by the ring of integers of $\mathbb{Q}(\sqrt{-3})$ or $\mathbb{Q}(\sqrt{-1})$, hence its Fourier coefficients $a_{f_{N,k}}(p)$ are zero when p is an inert prime (i.e. $p \equiv 2 \pmod 3$ or $p \equiv 3 \pmod 4$ respectively). Multiplicativity of the Fourier coefficients then implies the observation.

On the other hand $A = BT^{-1}B^{-1}$, therefore

$$\begin{aligned} f_{N,k}(2\tau/k)|_2 A = (f_{N,k}(2\tau/k)|_2 B)|_2 T^{-1}|_2 B^{-1} &= (\lambda_{k,N} f_{N,k}(2\tau/k)|_2 T^{-1})|_2 B^{-1} \\ &= \lambda_{k,N} \lambda_{k,N}^{-1} e^{-4\pi i/k} f_{N,k}(2\tau/k). \end{aligned}$$

□

Corollary 12. *We have that*

a) $\Delta_{N,k}(\tau) \in S_k(\Gamma_0(N))$,

b) $\Delta_{N,8}(\tau)^{1/2}|_4 A = -\Delta_{N,8}(\tau)^{1/2}$ *and* $\Delta_{N,8}(\tau)^{1/2}|_4 T = -\Delta_{N,8}(\tau)^{1/2}$,

c) $\Delta_{N,12}(\tau)^{1/2}|_6 A = -\Delta_{N,12}(\tau)^{1/2}$ *and* $\Delta_{N,12}(\tau)^{1/2}|_6 T = -\Delta_{N,12}(\tau)^{1/2}$.

We now recall some basic facts about Jacobians of modular curves. For more details see Chapter 6 of [8]. Denote by $Jac(X_k)$ the Jacobian of X_k. We will view it either as $S_2(\Gamma_k)^\wedge/H_1(X_k,\mathbb{Z})$ (where $\gamma \in H_1(X_k,\mathbb{Z})$ acts on $f(\tau) \in S_2(\Gamma_k)$ by $f(\tau) \mapsto \int_\gamma f(\tau)d\tau$), or as the Picard group $Pic^0(X_k)$ of X_k, which is the quotient $Div^0(X_k)/Div^l(X_k)$ of the degree zero divisors of X_k modulo principal divisors. If x_0 is a base point in X_k then X_k embeds into its Picard group under the Abel-Jacobi map

$$X_k \to Pic^0(X_k), \qquad x \mapsto (x) - (x_0),$$

where $(x) - (x_0)$ denotes the equivalence class of divisors $(x) - (x_0) + Div^l(X_k)$.

It is known that the parametrization $\Phi_k : X_k \to E_k$ can be factored as

$$X_k \hookrightarrow Jac(X_k) \xrightarrow{\psi_k} \tilde{E}_k \xrightarrow{\phi_k} E_k. \tag{7}$$

Here $X_k \hookrightarrow Jac(X_k)$ is the Abel-Jacobi map (for some base point $x_0 \in X_k$), ϕ_k is a rational isogeny, and $\tilde{E_k}$ (together with ψ_k) is the strong Weil curve associated to the newform $f_{N,k}(2\tau/k)$ via Eichler-Shimura construction as follows.

Let V_k be a $\mathbb{C}$-span of $f_{N,k}(2\tau/k) \in S_2(\Gamma_k)$, and define $\Lambda_k := H_1(X_k)|V_k$. Restriction to V_k gives a homomorphism ψ_k

$$Jac(X_k) \to V_k^\wedge/\Lambda_k \cong \tilde{E_k}.$$

Here $V_k^\wedge/\Lambda_k$ is a one-dimensional complex torus isomorphic to the rational elliptic curve $\tilde{E_k}$ with the Weierstrass equation $\tilde{E_k} : y^2 = x^3 - \frac{g_2(\Lambda_k)}{4}x - \frac{g_3(\Lambda_k)}{4}$.

Let S be either A or T. Since by Lemma 10 S normalizes Γ_k, we can define the action of S on $Jac(X_k)$ in two equivalent ways: for $\phi \in S_2(\Gamma_k)^\wedge/H_1(X_k,\mathbb{Z})$ and $f(\tau) \in S_2(\Gamma_k)$ let $S(\phi)(f(\tau)) := \phi(f(\tau)|_2 S)$, or for $P = (x) - (x_0) \in Pic^0(X_k)$ let $S(P) = (Sx) - (Sx_0)$. Now Lemma 11 implies that the action of S on $Jac(X_k)$ descends to the automorphism of $\tilde{E_k}$ of the order $\frac{k}{2}$.

Recall that x and y are functions on E_k satisfying Weierstrass equation $y^2 = f_k(x)$, and that $x(\tau) = x \circ \Phi_k(\tau)$ and $y(\tau) = y \circ \Phi_k(\tau)$ are modular functions on X_k.

Proposition 13. *Let S be either A or T. If $\Phi_k^{-1}(\mathcal{O})$ is invariant under A and T, then*

a)

$$x(\tau)|S = \begin{cases} x(\tau), & \text{if } k = 4, \\ -x(\tau), & \text{if } k = 8. \end{cases}$$

b)

$$y(\tau)|S = \begin{cases} y(\tau), & \text{if } k = 6, \\ -y(\tau), & \text{if } k = 12, \end{cases}$$

Proof. For $P \in E_k$, we define the $S(P) := \phi_k(S(\tilde{P}))$ for any $\tilde{P} \in \phi_k^{-1}(P)$. It is well defined since S-invariance of $\Phi_k^{-1}(\mathcal{O})$ implies the S-invariance of $Ker(\phi_k)$. We have that $\phi_k(S(P)) = S(\phi_k(P))$, hence S is an automorphism of E_k.

Let x_0 be a base point of Abel-Jacobi map in (7). Then $x_0 \in \Phi_k^{-1}(\mathcal{O})$, hence $\phi_k \circ \psi_k$ maps $(Sx_0) - (x_0)$ to $\mathcal{O}$ in E_k. In particular, for $x \in X_k$ we have

$$\Phi_k(Sx) = \phi_k \circ \psi_k((Sx) - (x_0)) = \phi_k \circ \psi_k((Sx) - (Sx_0)) = S(\Phi_k(x)). \tag{8}$$

Assume first that $k = 4$. Then $j(E_4) \neq 0, 1728$, and the automorphism group of E_4 is of order 2 generated by $(x, y) \mapsto (x, -y)$. In particular $x(S(P)) = x(P)$, for every $P \in E_4$.

If $k = 8$, then S is an automorphism of order $\frac{k}{2} = 4$ of $\tilde{E_k}$, hence $j(\tilde{E_k}) = 1728$, and $g_3(\Lambda_8) = 0$. Moreover ϕ_k is isomorphism (defined over $\mathbb{Q}$), which implies that S is an isomorphism of order 4 of E_8 as well. The automorphism group is generated by $(x, y) \mapsto (-x, iy)$, hence $x(S(P)) = -x(P)$ for every $P \in E_8$.

If $k = 6$ or 12, then $j(\tilde{E_k}) = 0$, $g_2(\Lambda_k) = 0$, and ϕ_k is an isomorphism (defined over $\mathbb{Q}$). Therefore, S has order 3 on E_k if $k = 6$, and order 6 if $k = 12$. The automorphism group is generated by $(x, y) \mapsto (e^{2\pi i/3}x, -y)$, and in particular $y(S(P)) = y(P)$ if $k = 6$, and $y(S(P)) = -y(P)$ if $k = 12$, for every $P \in E_k$.

Now (8) implies

$$x(\tau)|S = x(S\tau) = x(\Phi_k(S\tau)) = x(S(\Phi_k(\tau))) \quad \text{and} \quad y(\tau)|S = y(S\tau) = y(\Phi_k(S\tau)) = y(S(\Phi_k(\tau))),$$

and the claim follows from the previous paragraph.

□

We need the following technical lemma. Recall that $Q_k(\tau) := x(\tau)\Delta_{N,k}(\tau)^{4/k}$.

Lemma 14. *If $\partial_{N,k}(Q_k(\tau)) \in M_6^{mer}(\Gamma_0(N))$, then $Q_k(\tau) \in M_4^{mer}(\Gamma_0(N))$.*

Proof. As in the proof of Proposition 3, we have that $\partial_{N,k}(Q_k(\tau)) = \frac{k}{8\pi i}x'(\tau)\Delta_{N,k}(\tau)^{4/k} = \frac{k}{8\pi i}\frac{x'(\tau)}{x(\tau)}Q_k(\tau)$. Let S be either A or T. Then $(x(S\tau))' = x'(\tau)|_2 S$, and the invariance of $\frac{x'(\tau)}{x(\tau)}$ under S (hence under $\Gamma_0(N)$) follows from the fact that $x(\tau)$ is an eigenfunction for S, which follows from the proof of Proposition 13. □

Since $Q_k(\tau) := x(\tau)\Delta_{N,k}(\tau)^{4/k}$, the Theorem 7 for $k = 4$ and 8 now follows from a) and b) of Corollary 12 and a) of Proposition 13, while $k = 6$ and 12 case follows from $\partial_{N,k}(Q_k)(\tau) = y(\tau)\Delta_{N,k}(\tau)^{6/k}$ together with a) and c) of Corollary 12, b) of Proposition 13 and Lemma 14.

4. Example

Let

$$f_{19,4}(\tau) = \sum_{n=1}^{\infty} a(n)q^n = q + 2q^3 - q^5 - 3q^7 + q^9 + \cdots$$

be a unique newform in $S_2(\Gamma_0(76))$, and denote by $\Delta_{19,4}(\tau) = f_{19,4}(\tau/2)^2 \in S_4(\Gamma_0(19))$.

Set $\Gamma = \begin{pmatrix} \frac{1}{2} & 0 \\ 0 & 1 \end{pmatrix}^{-1} \Gamma_0(76) \begin{pmatrix} \frac{1}{2} & 0 \\ 0 & 1 \end{pmatrix}$. For $\tau \in \bar{\mathbb{H}}$ we define

$$\Psi(\tau) = \pi i \int_{i\infty}^{\tau} f(z/2)dz.$$

For $\gamma \in \Gamma$ and $\tau \in \bar{\mathbb{H}}$, define $\omega(\gamma) := \Psi(\gamma\tau) - \Psi(\tau)$. One easily checks that $\frac{d}{d\tau}\omega(\tau) = 0$, hence $\omega(\gamma)$ does not depend on τ. Denote by Λ the image of Γ under ω. By Eichler-Shimura theory Λ is a lattice, and $\Psi(\tau)$ induces a parametrization $X := \mathbb{H}/\Gamma \to \mathbb{C}/\Lambda$. The complex torus $\mathbb{C}/\Lambda$ is isomorphic to $E : y^2 = x^3 - \frac{g_2(\Lambda)}{4}x - \frac{g_3(\Lambda)}{4}$ by the map given by Weierstrass $\wp$-function and its derivative, $z \longmapsto (\wp(z,\Lambda), \wp'(z,\Lambda)/2)$, thus by composing these two maps we obtain a modular parametrization $\Phi : X \to E$.

One finds that generators ω_1 and ω_2 of Λ are

$$\omega_1 = 1.1104197465122\ldots, \quad \omega_2 = 0.5552098732561\ldots + 2.1752061725591\ldots \times i.$$

Moreover, $g_2(\Lambda) = \frac{256}{3}$ and $g_3(\Lambda) = \frac{4112}{27}$, hence it follows from Proposition 3 that

$$Q(\tau) = \Delta_{19,4}(\tau)\wp(\Psi(\tau),\Lambda) = 1 + \frac{1}{3}\left(8q + 8q^2 + 64q^3 + 232q^4 + 336q^5 + 256q^6 + 512q^7 + \cdots\right)$$

satisfies a differential equation

$$\partial_{19,4}(Q)^2 = Q^3 - \frac{64}{3}Q\Delta_{19,4}^2 - \frac{1028}{27}\Delta_{19,4}^3. \tag{9}$$

One finds that

$$GCD\left(\{p + 1 - a(p) : p \text{ prime}, p \equiv 1 \pmod{76}\}\right) = 1,$$

hence it follows from the special case of Drinfeld-Manin theorem (see Theorem 2.20 in [7]) that $\Psi(\tau)$ maps cusps of X to the lattice Λ, or equivalently that Φ maps cusps of X to the point at infinity of E. Modular curve X has six cusps, and one can check (for example by using software package Magma) that the degree of Φ is six, therefore the conditions of Proposition 5 and Theorem 7 are satisfied, and we conclude that $Q(\tau) \in M_4(\Gamma_0(19))$.

References

1 D. Abramovich, *A linear lower bound on the gonality of modular curves*, Internat. Math. Res. Notices (1996), no. 20, 1005–1011.

2 A. Atkin, J. Lehner, *Hecke operators on* $\Gamma_0(m)$, Math. Ann. 185 (1970) 134–160.

3 B. J. Birch, H. P. F. Swinnerton-Dyer, *Elliptic curves and modular functions*, Modular functions of one variable IV, Lecture Notes in Mathematics, 1975, Volume 476/1975, 2–32,

4 C. Breuil, B. Conrad, F. Diamond, R. Taylor, *On the modularity of elliptic curves over* $\mathbb{Q}$*: wild 3-adic exercises.* J. Amer. Math. Soc. 14 (2001), no. 4, 843–939 (electronic).

5 F. Brunault, *On the ramification of modular parametrization at the cusps*, arXiv:1206.2621v1

6 J. A. Csirik, J. L. Wetherell, M. E. Zieve *On the genera of* $X_0(N)$, arXiv:math/0006096v2

7 H. Darmon, *Rational points on modular elliptic curves*, CBMS Regional Conference Series in Mathematics, AMS, **101**, (2004)

8 F. Diamond, J. Shurman, *A first course in modular forms*, Graduate Texts in Mathematics, vol. 228, Springer-Verlag, New York, 2005.

9 B. Gross, D. Zagier, *Heegner Points and Derivatives of L-series*, Invent. Math. **84** (1986) pp. 225–320.

10 P. Guerzhoy, *The Ramanujan differential operator, a certain CM elliptic curve and Kummer congruences*, Compositio Mathematica, 141 (2005), no. 3, 583–590.

11 M. Kaneko, Y. Sakai, *The Ramanujan-Serre differential operators and certain elliptic curves*, preprint.

12 Y. Martin, K. Ono, *Eta-quotients and elliptic curves*, Proc. Amer. Math. Soc., **125** (1997), 3169–3176.

13 K. Ono, *The Web of Modularity: Arithmetic of the Coefficients of Modular Forms and q-series*, CBMS Regional Conference Series in Mathematics, AMS, **102**, (2003)

14 R. Taylor, A. Wiles, *Ring-theoretic properties of certain Hecke algebras.* Ann. of Math. (2) 141 (1995), no. 3, 553–572.

15 M. Watkins, *Computing the modular degree of an elliptic curve*, Experiment. Math. **11** (2002),no.4, 487–502.

Matija Kazalicki mkazal@math.hr
Department of Mathematics, University of Zagreb, Bijenicka cesta 30, Zagreb, Croatia

Yuichi Sakai dynamixaxs@gmail.com

Koji Tasaka k-tasaka@math.kyushu-u.ac.jp
Graduate school of mathematics, Kyushu University, 744 Motooka Nishiku, Fukuoka-city, Fukuoka, 819-0395 Japan