Communications in
Number Theory and Physics
Volume 16, Number 2, 353–400, 2022

Modular parametrization as Polyakov path integral: cases with CM elliptic curves as target spaces

Satoshi Kondo and Taizan Watari

For an elliptic curve E over an abelian extension k/K with CM by K of Shimura type, the L-functions of its $[k : K]$ Galois representations are Mellin transforms of Hecke theta functions; a modular parametrization (surjective map) from a modular curve to E pulls back the 1-forms on E to give the Hecke theta functions. This article refines the study of our earlier work and shows that certain class of chiral correlation functions in Type II string theory with $[E]_{\mathbb{C}}$ (E as real analytic manifold) as a target space yield the same Hecke theta functions as objects on the modular curve. The Kähler parameter of the target space $[E]_{\mathbb{C}}$ in string theory plays the role of the index (partially ordered) set in defining the projective/direct limit of modular curves.

AMS 2000 subject classifications: Primary81T40, 81T30, 11G15, 11G05, 11G40.

1. Introduction

In this article, we address a question whether the theory of modular parameterization has its avatar stated in the language of string theory. Prior to the ordinary Introduction in a paper in string theory starting in section 1.2, however, it is better to share the following pure mathematical facts in section 1.1.

As is often the case in math papers, we allow ourselves to use notations and jargon in the Introduction without enough explanations; we intend to provide appropriate explanations or references in later sections at least to the level minimally required by readers without background in arithmetic geometry.

arXiv: 1912.13294

1.1. The phenomenon that we are interested in, by way of example

Consider two elliptic curves:

$$E_{32A2} : \text{the closure of } \left\{(x,y) \mid y^2 = x^3 - x\right\},$$
$$E_{64A1} : \text{the closure of } \left\{(x,y) \mid y^2 = x^3 - 4x\right\}.$$

The j-invariants of the two elliptic curves are both equal to $j = 1728$, and indeed the two curves are isomorphic under the map $(x,y)_{E_{32A2}} \mapsto (x,y)_{E64A1} = (\sqrt{2}^3 y_{E_{32A2}}, \sqrt{2}^2 x_{E_{32A2}})$, when we allow arbitrary coefficients in $\mathbb{C}$ such as $\sqrt{2}$ in relating $(x,y)_{64A1}$ with $(x,y)_{32A2}$. That is, $[E_{32A2}]_{\mathbb{C}} \cong [E_{64A1}]_{\mathbb{C}}$. In arithmetic geometry, however, the two elliptic curves may be regarded different; in the category of algebraic varieties over the field $\mathbb{Q}$, the two elliptic curves are two different objects, in the sense that the $\mathbb{Q}$-algebra $\mathbb{Q}[x,y]/(x^3 - x - y^2)$ is not isomorphic to $\mathbb{Q}[x,y]/(x^3 - 4x - y^2)$.

The L-function is defined separately for E_{32A2} and for E_{64A1}, either by the Galois group action on the 1st cohomology groups of $E_{32A2} \otimes_{\mathbb{Q}} \overline{\mathbb{Q}}$ and $E_{64A1} \otimes_{\mathbb{Q}} \overline{\mathbb{Q}}$, or by counting the number of points in their reduction on the finite fields $\mathbb{F}_p$ for *rational primes*[1] p. They are[2]

$$\begin{aligned} L(E_{32A2}/\mathbb{Q}, s) &= 1 - \frac{2}{5^s} - \frac{3}{9^s} + \frac{6}{13^s} + \frac{2}{17^s} - \frac{1}{25^s} + \cdots, \\ L(E_{64A1}/\mathbb{Q}, s) &= 1 + \frac{2}{5^s} - \frac{3}{9^s} - \frac{6}{13^s} + \frac{2}{17^s} - \frac{1}{25^s} + \cdots. \end{aligned}$$

They are Mellin transforms of the following power series

$$f_{32A2}(\tau) = q - 2q^5 - 3q^9 + 6q^{13} + 2q^{17} - q^{25} + \cdots, \tag{1}$$
$$f_{64A1}(\tau) = q + 2q^5 - 3q^9 - 6q^{13} + 2q^{17} - q^{25} + \cdots, \tag{2}$$

[1] A rational prime is a jargon in number theory that just means a prime integer in $\mathbb{Z}$ such as $p = 2, 3, 5, 7, \cdots$ for people in all other fields. We will also use the word *prime integer* for the same meaning in this manuscript.

[2] For a rational prime p (except $p = 2$ in the case of E_{32A2} and E_{64A1}), the coefficient a_p of the p^{-s} term in $L(E/\mathbb{Q}, s)$ is $p+1-\#(E \otimes_{\mathbb{Q}} \mathbb{F}_p)$, where $\#(E \otimes \mathbb{F}_p)$ is the number of points in the reduction $E \otimes \mathbb{F}_p$ including the (∞, ∞) point. For example, $E_{32A2} \otimes \mathbb{F}_5$ consists of 8 points $(x,y) = (0,0)$, $(\pm 1, 0)$, $(2, \pm 1)$, $(3, \pm 2)$ and (∞, ∞), so $a_{p=5} = (5+1) - 8 = -2$, while $E_{64A1} \otimes \mathbb{F}_5$ consists of 4 points $(x,y) = (0,0)$, $(2,0)$, $(3,0)$ and (∞, ∞), so $a_{p=5} = (5+1) - 4 = +2$.

where $q = e^{2\pi i\tau}$, with τ in the upper half complex plane $\mathcal{H}$; the Mellin transformation is with respect to the imaginary part $t \in \mathbb{R}_{>0}$ of τ, $\tau = it$. Now, a highly non-trivial fact is that $f_{32A2}(\tau)$ and $f_{64A1}(\tau)$ are both modular forms of weight-2 for the group $\Gamma_0(64) \subset \mathrm{SL}(2;\mathbb{Z})$, where the group $\mathrm{SL}(2;\mathbb{Z})$ acts on $\tau \in \mathcal{H}$ through the linear fractional transformation.

The theory of modular parametrization attributes this non-trivial fact to another non-trivial fact illustrated in the following. First, as explained in many textbooks, the modular curve $X_0(64)$—the compact Riemann surface obtained as the closure of $\Gamma_0(64)\backslash\mathcal{H}$—is regarded as a projective algebraic variety that uses only coefficients in $\mathbb{Q}$ in its defining equations. To be very explicit, one may use three linearly independent weight-2 cusp forms of $\Gamma_0(64)$,

$$\begin{aligned}
X_1(\tau) &= q - 3q^9 + 2q^{17} - q^{25} + 10q^{41} - 7q^{49} - 12q^{65} + \cdots, \\
X_2(\tau) &= q^2 - 2q^{10} - 3q^{18} + 6q^{26} + 2q^{34} - q^{50} - 10q^{58} + \cdots, \\
X_5(\tau) &= 2\left(q^5 - 3q^{13} + 5q^{29} + q^{37} - 3q^{45} - 7q^{53} + 5q^{61} + \cdots\right)
\end{aligned}$$

to construct a map

$$\Phi_{|K|} : X_0(64) \ni \Gamma_0(64)\cdot\tau \mapsto [X_1 : X_2 : X_5] = [X_1(\tau) : X_2(\tau) : X_5(\tau)] \in \mathbb{C}P^2.$$

The image of this map is

$$C := \left\{[X_1 : X_2 : X_5] \in \mathbb{P}^2 \mid X_1^3X_5 + X_1X_5^3 - 2X_2^4 = 0\right\}; \tag{3}$$

the algebraic variety C is defined over $\mathbb{Q}$, and is regarded[3] as an arithmetic model of $X_0(64)$ over $\mathbb{Q}$. Secondly, there exist surjective maps $\nu'_{32A2} : C \to E_{32A2}$ and $\nu'_{64A1} : C \to E_{64A1}$ sending $[X_1 : X_2 : X_5] \in C$ to[4]

$$(x,y)_{32A2} = \left(\frac{(X_1+X_5)^2}{4X_2^2},\ -\frac{(X_1-X_5)^2(X_1+X_5)}{8X_2^3}\right),$$

$$(x,y)_{64A1} = \left(\frac{X_1^2+X_5^2}{X_2^2},\ -\frac{(X_1-X_5)(X_1^2+X_5^2)}{X_2^3}\right);$$

[3]The notion of an *arithmetic model* is explained in section 2.1.2. The map $\Phi_{|K|}$ being an isomorphism follows from the facts that (i) both $X_0(64)$ and C are curves of genus 3, and (ii) C is non-singular.

[4]Note that $(x_{32A2})^3 - x_{32A2} - (y_{32A2})^2 = 0$ and $(x_{64A1})^3 - 4x_{64A1} - (y_{64A1})^2 = 0$, when one uses $X_1^3X_5 + X_1X_5^3 - 2X_2^4 = 0$.

it should be noted that those maps involve only coefficients in $\mathbb{Q}$ (it is said that such a map is *defined over* $\mathbb{Q}$; such notations as $C \to_{/\mathbb{Q}} E$ or $C/\mathbb{Q} \to_{/\mathbb{Q}} E/\mathbb{Q}$ are used to emphasize that aspect). It is now straightforward to see that

$$\begin{aligned}
\nu'_{32A2} \circ \Phi_{|K|} : \mathcal{H} \ &\ni \tau \longmapsto (x,y)_{32A2} \in [E_{32A2}]_{\mathbb{C}}, \\
&\begin{cases} x_{32A2} = q^{-2}/4 + q^2 + q^6/2 + \cdots \\ y_{32A2} = -q^{-3}/8 + q/4 + 7q^5/8 + \cdots \end{cases} \\
&\frac{1}{2\pi i} \left(\nu'_{32A2} \circ \Phi_{|K|}\right)^* \left(\frac{dx}{4y}\right) = d\tau f_{32A2}(\tau), \\
\nu'_{64A1} \circ \Phi_{|K|} : \mathcal{H} \ &\ni \tau \longmapsto (x,y)_{64A1} \in [E_{64A1}]_{\mathbb{C}}, \\
&\begin{cases} x_{64A1} = q^{-2} + 2q^6 - q^{14} + \cdots \\ y_{64A1} = -q^{-3} + 2q - q^5 + 2q^9 + \cdots \end{cases} \\
&\frac{1}{2\pi i} \left(\nu'_{64A1} \circ \Phi_{|K|}\right)^* \left(\frac{dx}{2y}\right) = d\tau f_{64A1}(\tau).
\end{aligned}$$

It is non-trivial that there exists a surjective map defined over $\mathbb{Q}$ from modular curves to elliptic curves such as E_{32A2} and E_{64A1}. Once such a map is found,[5] the Galois group $\mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})$ acts on both sides of the pullback $(\nu')^* : H^1_{et}(E \otimes \overline{\mathbb{Q}}, \overline{\mathbb{Q}}_\ell) \to H^1_{et}(C \otimes \overline{\mathbb{Q}}, \overline{\mathbb{Q}}_\ell)$ in a way that commutes with $(\nu')^*$. Now, the L-function of E is translated into the language of Galois group action on $H^1_{et}(C \otimes \overline{\mathbb{Q}}, \overline{\mathbb{Q}}_\ell) \cong H^1(X_0(64), \mathbb{C})$; the correspondence between the L-function and a modular form is not a non-trivial phenomenon for those with some training in arithmetic geometry then (the Eichler–Shimura theory).

The presentation so far is an example of a theory by Deuring [8] formulated in a more modern language of the Eichler–Shimura theory. Deuring's theory was for all elliptic curves with complex multiplications whose j-invariants are in $\mathbb{Q}$. Deuring's theory has been generalized/extended in multiple directions since then. One direction is for cases of elliptic curves not necessarily with complex multiplication but still with rational j-invariants, widely known for its relevance to Fermat's theorem and the Shimura–Taniyama conjecture, now a theorem [1]. Another direction is to relax the condition $j \in \mathbb{Q}$ somewhat, while still restricting attention to those with complex multiplication [26]; in this direction, a solid theory is available for a class of elliptic curves, which we call elliptic curves of Shimura-type in this article.

[5] then there are infinitely many of them; $(\nu' \circ \Phi_{|K|})^*(dx/y) \propto d\tau f_E(\tau)$ for all those maps ν' defined over $\mathbb{Q}$.

In this article, we will make an attempt at digesting the theory of modular parametrization for elliptic curves of Shimura type by using the language of string theory.

1.2. Questions to ask from string-theory perspectives

With a most naive look at the phenomenon described in section 1.1, one finds that a modular form pops up when arithmetic data in a geometry are organized in an appropriate way. Although mathematical proof has been established for the phenomenon for certain class of cases, the origin of the modular transformation remains unclear, and the variable τ of the modular forms such as the inverse Mellin transforms of $L(E_{32A2}/\mathbb{Q}, s)$ and $L(E_{64A1}/\mathbb{Q}, s)$ are nothing more than a dummy variable to organize arithmetic data.[6] Incidentally, when geometry is dealt with by a string theory, correlation functions on genus-1 worldsheet have to have invariance/covariance under the modular transformation on the complex structure parameter τ_{ws} of the genus-1 worldsheet. It is natural to wonder if there is any relation between the modular forms that are dual to the L-functions and some correlation functions in string theory. In this article, we follow the spirit of [23] [22] and [16], and pursue this question.

If any relation of that kind is to be established, there has to be a clear statement on the following two issues, hopefully three. First, L-functions are defined for individual arithmetic models, whereas string theory deal with geometry over $\mathbb{C}$. For example, elliptic curves E_{32A2} and E_{64A1} have different L-functions and corresponding modular forms, but both are regarded just as one common complex analytic elliptic curve $[E_{z=i}]_{\mathbb{C}}$ where $j(z) = 1728$. How can string theory with the target space $[E_z]_{\mathbb{C}}$ contain information of data of multiple different arithmetic models of $[E_z]_{\mathbb{C}}$?

Secondly, string theory (worldsheet conformal field theory (CFT)) can be specified only after fixing not just the complex structure of a target space but also its complexified Kähler parameter. So, individual correlation functions in string theory are for specific choices of a Kähler parameter; on the other hand, the definition of L-functions only involve defining equations of the geometry, not a metric. If there is a relation between the correlation functions and the L-functions, how does the dependence on the choice of Kähler metric in the former go away in the latter?

[6]The modular curve $X_0(N)$ may be regarded as a moduli space of an abstract complex 1-dimensional torus T^2 with level-N structure, so the argument τ may be interpreted as the modulus of the T^2 in this context. It is still hard to find a motivation for probing such varieties as E_{32A2} and E_{64A1} with the modular curves.

In this article, we find that the modular forms associated with certain class of arithmetic models of $[E_z]_{\mathbb{C}}$ are obtained as appropriate linear combinations[7] of the class of chiral correlation functions (see explanations around (11) in section 2.2.2)

$$f^{\mathrm{II}}_{1\Omega'}(\tau_{ws};\beta) := \frac{-i}{2\pi}\sqrt{\frac{2}{\alpha'}}\mathrm{Tr}^{\mathrm{Rmnd}}_{V_\beta}\left[Fe^{\pi i F} q_{ws}^{L_0-\frac{c}{24}}(\partial_u X^{\mathbb{C}})(u)\right] \tag{11}$$

in $[E_z]_{\mathbb{C}}$-target SCFT's; the appropriate linear combination is given by the formula (31). Infinitely many correlation functions are available in a family of string theory with a given $[E_z]_{\mathbb{C}}$ and varying choices of complexified Kähler parameters, and those infinitely many correlation functions are organized to obtain the L-functions of infinitely many arithmetic models of $[E_z]_{\mathbb{C}}$. So, the two issues above are resolved simultaneously. The complexified Kähler parameter plays the role of the partially ordered set parametrizing worldsheet CFT's, their correlation functions, modular curves, and their cohomology groups (see the Observation 4 in section 4.3).

The third issue is this: it is desirable if a systematic description of the relation between the L-functions and string correlation functions include (a) string theory interpretation of the argument τ, (b) clear formulas on the level N of the modular groups such as $\Gamma_0(N)$, (c) relation to the theory of modular parametrization.

Presentation in this article has a clear statement about the issues (a) and (b), improving similar statements already made in [16]. The argument τ corresponds to $\tau_{ws}/N_{D\Lambda}$, where τ_{ws} is the complex structure parameter of the $g = 1$ worldsheet in string theory; the integer $N_{D\Lambda}$ is associated with the conductor of arithmetic models on one hand (arithmetic geometry), and with the Kähler metric on the other (string theory); see (8, 15, 30) for more. So, the modular transformation is interpreted as that of the homology classes of the $g = 1$ worldsheet in string theory. Let us comment on the issue (c) in section 1.3.

1.3. Summary and discussions

Summary (continued) Already half of the take-away messages of this article are contained in section 1.2. So, let us touch upon a few other observations in this article here.

One of those observations is that a subgroup of the automorphism group of the fusion algebra in the string theory (rational SCFT) in question has a

[7] by following [16], but in a more polished-up way

role to play (see the Observation 2 in section 3.2 and the examples in section 3.3). We call it the CM group because the subgroup has an interpretation as complex multiplication operations of the target space. The idea that we should focus on this subgroup comes from perspectives in arithmetic geometry, as we explain in the preprint version of this article [17, §3.1] (omitted from this journal version). This observation may also be seen as an inspiring idea on a more general question on structure of arithmetic characterizations in the vector space of general chiral correlation functions of rational CFT's (e.g., [14]).

Another observation that deserves attention (the Observation 3) is that correspondence with objects in arithmetic geometry is made possible in the formula (31) after we allow ourselves to take linear combinations of chiral correlation functions of multiple different target spaces. Here, we are not talking of a set of target spaces for which there is no justification, but of the set of target spaces between which there are Galois group action. This is actually a very natural thing to do from the perspective in arithmetic geometry, as we will explain in section 4.2 (and also section 2.1.4). This observation can be seen as an example of getting a transparent picture by occasionally relaxing ordinary norms in quantum field theory.

Discussion and Open Questions To what extent the mathematical relation (31) between the correlation functions in string theory and L-functions in arithmetic geometry is just an accidental agreement, or to what extent the relation manages to grasp the phenomenon in section 1.1 at its core/essence in the language of string theory? The issue (c) at the end of section 1.2 points to this question. That is not a well-defined question in the absence of evaluation criteria, but is still an important question in guiding our thoughts.

There are two arguments in favor of thinking that the relation may be something more than accidental agreement of two mathematical objects. One is that both the modular forms characterized by the Galois representations of arithmetic models and the chiral correlation functions are regarded as holomorphic 1-forms on the target space pulled back by maps that are central to the theory of modular parametrization on one hand, and to the Polyakov path-integral formulation on the other. The other argument is that there are well-motivated and natural ways to think of those pulled back objects as those on modular curves in both of the theory of modular parametrization and in the discussion developed in this article (see the Observation 1 in sections 3.1). The triangle diagram (16) schematically describes that. The discussion in this article captures lot of structure in the language of string theory of what is going on in the theory of modular parametrization of elliptic curves with complex multiplication. See also $\diamondsuit$ below.

Many questions also remain, which are beyond the scope of this article. The first obvious question is whether the discussion can be applied to geometry other than elliptic curves. Another question is whether there is a special property in the worldsheet SCFT when the target space allows arithmetic model. For example, it is known on the side of arithmetic geometry that an elliptic curve defined over $\mathbb{Q}$ has an associated modular form of weight-2, regardless of whether it has complex multiplication or not; if the story in this article has a generalization to all the elliptic curves with arithmetic models, then one has to find a special property in their stringy treatments (CFT's) as well, from which the appropriate modular form(s) can be extracted. Finally, there is another question that may be related to the questions raised so far. In the case of a CM elliptic curve as the target space, we presented the key objects $f^{\rm II}_{1\Omega'}(\tau_{ws}; \beta)$ as chiral correlation functions in the rational SCFT; the same objects are obtained also as open string correlation functions, when β's are identified with D0-type Cardy states [13]. Which interpretation allows generalization to the cases with target space geometries other than CM elliptic curves? We have not made an attempt at resolving these different interpretations.

1.4. Reading guide

0. The core materials in this article are the Observations 1–4 and the Formula (31) in section 4.1. It is an option to skip the math-heavy sections 2.1.3 and 2.1.4 at the first reading and visit there later when really necessary. Not much is lost by not following the examples in detail; they are served just for illustration purposes.

Notations and minimal list of facts on modular forms are collected in the appendix.

1. We regard that this manuscript submitted to CNTP and the preprint [17] are the same article; the same scientific achievements are presented in different styles. We refer to this version as the journal version, while the preprint [17] is called the preprint version. The primary achievement of this article is to establish a string-theory language version of the phenomenon in section 1.1 loosely referred to as theory of modular parametrization. That achievement is seen as an output in string theory, rather than in arithmetic geometry. So, we set string theorists as the primary audience in this journal version. Some materials in the preprint version are omitted in this version, when they are too much or too distracting for ordinary string theorists, while a little more expository materials on arithmetic geometry and algebraic number theory are included here so that the expected audience do not have to go through many literatures to follow this journal version.

Here is the list of major difference between the two versions, stated in more concrete terms.

- ♠ The relation between the string-theory chiral correlation functions and the L-functions of the arithmetic models of the target spaces is stated in the preprint version more comprehensively (covering both newforms and oldforms) along with the derivation ([17, §3.3]). In this journal version, only just one key result for newforms is stated in the form of a formula, and all the rest are omitted.
- ♣ The theory of modular parametrization for elliptic curves of Shimura-type is presented in this journal version as a review in section 2.1.4. On the other hand, the preprint version does not avoid using the language and logic of arithmetic geometry at all to explain systematically how the Galois representations associated with those curves correspond to modular forms. The materials in the preprint version [17, §4.1.3, 4.1.4] are close parallel of discussions in existing literatures [28] for a similar (but not the same) class of curves; we still had to fully write up and present the discussion at least once somewhere for the class of curves we need to deal with in these two versions, so we did that in the preprint version.
- ♢ There are two different sets of literatures in string theory that discuss Galois group action in the context of string theory. One is to look for relations between string-theory observables and L-functions of Galois representations (e.g., [23], [22], [2], [16], [15]), and the other to study how Galois group may act on the data of rational CFT/modular tensor category (e.g., [5], [3], [10], [11], [6], [7], [4], [14]). The authors are unaware of literatures trying to bring both into a unified framework. The preprint version [17, §5] did it, which is made possible after managing to tell the story of the observables–L-functions connection in the language of modular curves (the Observation 1 in section 3.1). We gave up including those materials in this journal version; an alternative might have been to expand the 7 pages of [17, §5] to something more than 20 pages to make it comprehensible to string theory community.[8]

[8]Already large fraction of the 7 pages in the preprint version was expository, and only small fraction was necessary to add a new observation unifying both stories. In a 20-page version, that ratio would only get worse.

♡ The notion of arithmetic models, and classifications of elliptic curves of Shimura-type over proper subfields of $\mathbb{C}$ are crucial elements in this article. The preprint version does not have a review of the two subjects, and just referred to the reviews that we wrote in an earlier publication [16] and to literatures/textbooks. In this journal version, however, we decided to include them, so it is easier for string theorists to read.

2. Theoretical developments in this article are built on our earlier publication [16]. The preprint version [17] is written as an ordinary journal article in this respect, in that we explained there explicitly which parts are additional achievements beyond the earlier publication [16], and which are not. Frequent remarks on such aspects, however, may also be distracting for audience who wish to focus on the main story/idea. So, in this journal version, we put down the main story/idea simply in the updated understanding of ours without referring too much about the difference from [16].

3. Difference between the approach of [23] and that of [16], [17] is explained already in [16, §4.3]. Readers interested more in the difference may also contact the authors for more explanations.

2. Preliminaries

This section contains only expository materials.

2.1. Math preliminaries

It is like a typical style of math papers to collect all preliminary information in an earlier section, but we could have explained various concepts and facts in this section 2.1 one by one at places where they are used. It is an option to skip section 2.1 (or sections 2.1.3–2.1.4) at the first reading, and come back when necessary.

When a reader finds that the following explanations are not enough,[9] appropriate resources to look at will be

- for sections 2.1.1 and 2.1.2, textbooks containing such key words as elliptic curves, class field theory, complex multiplication.
- For section 2.1.3, see [16, §4.2] and references therein.
- For section 2.1.4, see the preprint version [17, §4.1].

[9] We admit that even sections 2.1.1 and 2.1.2 are written as a list of facts, not as an explanation.

2.1.1. CM elliptic curves as complex analytic manifolds An elliptic curve as a complex analytic manifold is described as the quotient space $[E_z]_{\mathbb{C}} = \mathbb{C}/(\mathbb{Z} + z\mathbb{Z})$ with a parameter $z \in \mathcal{H}$ determining its complex structure. To be more precise, it is the SL(2; $\mathbb{Z}$) orbit, $\mathrm{SL}(2;\mathbb{Z}) \cdot z \subset \mathcal{H}$, that specifies an elliptic curve as a complex analytic manifold. An elliptic curve $[E_z]_{\mathbb{C}}$ is said to *have complex multiplication*,[10] when the ring $\mathrm{End}([E_z]_{\mathbb{C}})$ of holomorphic maps $[E_z]_{\mathbb{C}} \to [E_z]_{\mathbb{C}}$ compatible with the abelian group law on $\mathbb{C}$ is strictly larger than the ring $\mathbb{Z}$.

It is known, for an elliptic curve $[E_z]_{\mathbb{C}}$ of CM type, that there is a set of mutually prime integers (a_z, b_z, c_z) such that

$$a_z z^2 + b_z z + c_z = 0, \qquad a_z, c_z > 0, \quad b_z^2 - 4a_z c_z < 0;$$

the SL(2; $\mathbb{Z}$) orbit of such a z corresponds to the SL(2; $\mathbb{Z}$) orbit of the even quadratic positive definite form given by the matrix

$$\begin{bmatrix} 2a_z & b_z \\ b_z & 2c_z \end{bmatrix}.$$

The field of fractions of the ring $\mathrm{End}([E_z]_{\mathbb{C}})$ is isomorphic to an imaginary quadratic field $K = \mathbb{Q}(z)$. One may factor out the square of integers as much as possible from the discriminant of the quadratic equation above into the form of

$$b_z^2 - 4a_z c_z = f_z^2 D_K, \qquad f_z \in \mathbb{N}_{>0},$$

so that $D_K < 0$ is free of the square of an odd prime integer, and is either (i) $D_K \equiv -3 \mod 4$ or (ii) $4|D_K$ but $16 \not| D_K$ (such as $D_K = -4$, -8, -20 etc.). The negative value D_K determined this way is the *discriminant of the imaginary quadratic field* K. The ring $\mathrm{End}([E_z]_{\mathbb{C}})$ is isomorphic to $\mathcal{O}_{f_z} := \mathbb{Z} \oplus \mathbb{Z} f_z w_K \subset K$, where $w_K := (1 + \sqrt{D_K})/2$ in the case (i) and $w_K := \sqrt{D_K}/2$ in the case (ii).

CM elliptic curves $[E_z]_{\mathbb{C}}$ (as complex analytic manifolds, over $\mathbb{C}$) are therefore classified first by their imaginary quadratic fields K (equivalently by the discriminant D_K), and then by f_z. The set of such CM elliptic curves sharing K and f_z (and hence the subring $\mathrm{End}([E_z]_{\mathbb{C}}) \cong \mathcal{O}_{f_z} \subset K$) is denoted

[10] One also says that $[E_z]_{\mathbb{C}}$ *is of CM-type*, and such an elliptic curve is referred to as a *CM elliptic curve*. We also sometimes include the information of the endomorphism ring $\mathrm{End}([E_z]_{\mathbb{C}})$ or its field of fractions K, and say that $[E_z]_{\mathbb{C}}$ *has complex multiplication by (*ring*)* or *by (*field*)*.

by $\mathcal{E}ll(\mathcal{O}_{f_z})$ (where the choice of K is implicit). The cardinality of this set is denoted by $h(\mathcal{O}_{f_z})$, and is called the *class number*. CM elliptic curves $[E_{z_a}]_{\mathbb{C}}$ in $\mathcal{E}ll(\mathcal{O}_{f_z})$, where $a = 1, \cdots, h(\mathcal{O}_{f_z})$, are regarded as $\mathbb{C}/\mathfrak{b}_{z_a}$ where $\mathfrak{b}_{z_a} := \mathbb{Z} + \mathbb{Z}z_a$. The lattices $a_{z_a}\mathfrak{b}_{z_a}$ $(a = 1, \cdots, h(\mathcal{O}_{f_z}))$ are invertible ideals of the ring $\mathcal{O}_{f_z}$; the set $\mathcal{E}ll(\mathcal{O}_{f_z})$ is in one to one with an abelian group $\mathrm{Cl}_K(\mathcal{O}_{f_z})$ called the ideal class group,[11] where $[E_{z_a}]_{\mathbb{C}}$ corresponds to the ideal class represented by the ideal $\mathfrak{b}_{z_a}$.

Example 2.1.1. For $(K, f_z) = (\mathbb{Q}(\sqrt{-4}), 1)$, $(\mathbb{Q}(\sqrt{-3}), 1)$, $(\mathbb{Q}(\sqrt{-8}), 1)$ and $(\mathbb{Q}(\sqrt{-4}, 2)$, the set $\mathcal{E}ll(\mathcal{O}_{f_z})$ and the group $\mathrm{Cl}_K(\mathcal{O}_{f_z})$ consist of just 1 element. $h(\mathcal{O}_{f_z}) = 1$. We can choose $z = i$, $(1 + \sqrt{3}i)/2$, $\sqrt{2}i$ and $2i$ for those cases, respectively.

For $(\mathbb{Q}(\sqrt{-20}), 1)$, on the other hand, $\mathcal{E}ll(\mathcal{O}_{f_z}) \cong \mathrm{Cl}_K(\mathcal{O}_{f_z})$ consists of two elements.

$$[E_{z_0}]_{\mathbb{C}} = \mathbb{C}/(\mathbb{Z} + w_K\mathbb{Z}), \quad \text{and} \quad [E_{z_1}]_{\mathbb{C}} = \mathbb{C}/(\mathbb{Z} + 2^{-1}(1 + w_K)\mathbb{Z}) \tag{4}$$

are not mutually isomorphic as complex analytic manifolds, but are both characterized by $(K, f_z) = (\mathbb{Q}(\sqrt{-20}), 1)$. They correspond to the ideal classes represented by $\mathfrak{b}_{z_0} = \mathcal{O}_{f_z=1} = (1)_{\mathcal{O}_{f_z=1}}$ and $2\mathfrak{b}_{z_1} = \langle 2, 1 + w_K \rangle \subset \mathcal{O}_{f_z=1}$ in the abelian group $\mathrm{Cl}_K(\mathcal{O}_{f_z=1}) \cong \mathbb{Z}/2\mathbb{Z}$, respectively, where ideals in the latter class (the non-trivial element of the group $\mathbb{Z}/2\mathbb{Z}$) such as $2\mathfrak{b}_{z_1}$ are not principal ideals (see also footnote 37).[12] •

[11]In this journal version, it will be possible to follow the main ideas and observations without knowing the global class field theory; this version does not provide precise definitions of such jargon as the ideal class group and ring class field, but is probably readable for the most part by just knowing that they are some kind of a group and a number field, respectively. It will be still easier to follow the discussion by knowing the fact that there is a canonical one-to-one correspondence between the set $\mathcal{E}ll(\mathcal{O}_{f_z})$ and the abelian group $\mathrm{Cl}_K(\mathcal{O}_{f_z})$ called the *ideal class group*; each element of $\mathrm{Cl}_K(\mathcal{O}_{f_z})$ is a class of ideals of the ring $\mathcal{O}_{f_z}$ represented by an ideal of $\mathcal{O}_{f_z}$. We will also use a fact that there is a canonical isomorphism between the abelian groups $\mathrm{Cl}_K(\mathcal{O}_{f_z}) \cong \mathrm{Gal}(L_{f_z}/K)$.

An exception is section 4.2.1 in this version, but readers may just skip section 4.2.1. This section, especially footnote 37, intends to provide to stringy readers with hands-on experience in the class field theory, while we explain how to use the formula (31) in practice.

In the preprint version [17], on the other hand, we assume that readers do not have troubles in following calculations involving algebraic number theory; so section 4.2.1 and footnote 37 may be useful when reading the preprint version §3.3 and 3.4 line by line.

[12]notations: For a ring R and its elements $x, y, z, \cdots \in R$, $(x)_R$ denotes the ideal

It is known that the j-invariant of a CM elliptic curve is always in the field of algebraic numbers $\overline{\mathbb{Q}}$. For example,

$$\begin{aligned} j(z)|_{z=i} &= 1728, \qquad j(z)|_{z=(1+\sqrt{3}i)/2} = 0, \\ j(z)|_{z=\sqrt{2}i} &= 8000, \qquad j(z)|_{z=2i} = 287496, \end{aligned}$$

$$\left(j(z)|_{z=\sqrt{5}i},\ j(z)|_{z=(1+\sqrt{5}i)/2}\right) = \left(320(1975+884\sqrt{5}),\ 320(1975-884\sqrt{5})\right). \tag{5}$$

It is further known that (a) the algebraic extension $K(j(z))$ over K is always an abelian extension of degree $[K(j(z)) : K] = h(\mathcal{O}_{f_z})$, and (b) $K(j(z)) \cong K(j(z'))$ when both $[E_z]_\mathbb{C}$ and $[E_{z'}]_\mathbb{C}$ are in the same set $\mathcal{E}ll(\mathcal{O}_{f_z})$. So, this extension field is uniquely determined by K and f_z and is called the *ring class field* L_{f_z}; in the case of $f_z = 1$, this field is called the *Hilbert class field* and is denoted by H_K. The abelian Galois group $\mathrm{Gal}(L_{f_z}/K)$ is known to be isomorphic to the abelian group $\mathrm{Cl}_K(\mathcal{O}_{f_z})$, and acts on the set of algebraic numbers $\{j(z_a) \mid [E_{z_a}]_\mathbb{C} \in \mathcal{E}ll(\mathcal{O}_{f_z})\}$ transitively.

The field extension $L_{f_z}/\mathbb{Q}$ is always Galois; the exact sequence

$$1 \longrightarrow \mathrm{Gal}(L_{f_z}/K) \longrightarrow \mathrm{Gal}(L_{f_z}/\mathbb{Q}) \longrightarrow \mathrm{Gal}(K/\mathbb{Q}) \longrightarrow 1$$

splits, where the generator of $\mathrm{Gal}(K/\mathbb{Q})$ lifts to the complex conjugation operation on L_{f_z} in $\mathrm{Gal}(L_{f_z}/\mathbb{Q})$. It is also known that $j(z_a)$ is real valued if and only if $[E_{z_a}]_\mathbb{C}$ in the set $\mathcal{E}ll(\mathcal{O}_{f_z})$ corresponds to a 2-torsion element[13] in the abelian group $\mathrm{Cl}_K(\mathcal{O}_{f_z})$.

2.1.2. Arithmetic models and the field of definitions Any elliptic curve $[E_z]_\mathbb{C} = \mathbb{C}/(\mathbb{Z}+z\mathbb{Z})$ as a complex analytic manifold can be embedded into $\mathbb{P}^2$ by using the Weierstrass $\wp$ function of $[E_z]_\mathbb{C}$, where the image is given by a cubic defining equation in $\mathbb{P}^2$. The image, regarded as an algebraic variety, is also denoted by $[E_z]_\mathbb{C}$.

---

of the ring R generated by one element x, while $\langle y, z, \cdots \rangle$ is an ideal generated by the set of elements in $\langle \quad \rangle$. Sometimes the subscript $_R$ is omitted, when that is obvious from the context.

[13] All the j-invariants in (5) are real valued. This is understood from the fact that the group $\mathrm{Cl}_K(\mathcal{O}_{f_z})$ is either trivial $\{0\}$ or $\mathbb{Z}/2\mathbb{Z}$ for all of $(K, f_z) = (\mathbb{Q}(\sqrt{-4}), 1)$, $(\mathbb{Q}(\sqrt{-3}, 1)$, $(\mathbb{Q}(\sqrt{-8}), 1)$, $(\mathbb{Q}(\sqrt{-4}), 2)$ and $(\mathbb{Q}(\sqrt{-20}), 1)$ (see Example 2.1.1).

In the following, let us introduce the notion of arithmetic models of an algebraic variety. That notion looks absolutely irrelevant to string theory as long as we focus on string theory in its formulation we know today, but it is central in arithmetic geometry. Because the underlying theme in [16] and this article is in exploring possibility for such notions in arithmetic geometry to play some role in string theory in the future, we do not throw away the notion of arithmetic models right away, but will review some of basic concepts in arithmetic geometry in sections 2.1.2–2.1.4.

For an algebraic variety $X_{\mathbb{C}}$ in a complex projective space, it may happen that one can choose all the coefficients of the defining equations in *a number field*[14] k. One may then think of a variety in the projective space with the field k, which is denoted by X_k. In such a case, X_k is said to be an *arithmetic model of* $X_{\mathbb{C}}$, and k the *field of definition of the arithmetic model* X_k. One may write $X_{\mathbb{C}} \cong X_k \otimes_k \mathbb{C}$ or $X_{\mathbb{C}} \cong X_k \times_k \mathbb{C}$ to refer to the relation between $X_{\mathbb{C}}$ and X_k. One also says[15] that X_k *is defined over* k, and $X_{\mathbb{C}}$ is the *base change of* X_k. When we wish to refer to an elliptic curve $[E_z]_{\mathbb{C}}$ as an object classified modulo isomorphisms over $\mathbb{C}$ (i.e., as a complex analytic manifold, or as a complex algebraic variety), we sometimes call it an elliptic curve *(defined) over* $\mathbb{C}$.

A pair of arithmetic models X_k and X'_k of a given $X_{\mathbb{C}}$ with a common field of definition k are regarded different when one cannot find an isomorphism between X_k and X'_k without allowing maps that involve coefficients outside of k. For example, two elliptic curves E_{32A2} and E_{64A1} are both defined over $\mathbb{Q}$, and are both arithmetic models of the same elliptic curve $[E_{z=i}]_{\mathbb{C}} = \mathbb{C}/(\mathbb{Z} + (z = i)\mathbb{Z})$ defined over $\mathbb{C}$. The two arithmetic models over $\mathbb{Q}$ are not the same model over $\mathbb{Q}$. In general, $X_{\mathbb{C}}$ does not necessarily have an arithmetic model in a designated number field $k \subset \overline{\mathbb{Q}}$; even when there is one for a given k, arithmetic models over k of a given $X_{\mathbb{C}}$ are not necessarily unique (as we have seen in an example).

For a CM elliptic curve $[E_z]_{\mathbb{C}}$, there is always an arithmetic model with a field of definition k, if k contains the number field $\mathbb{Q}(j(z))$; to see this, it is enough to note that the elliptic curve[16]

[14]A subfield k of the complex number field $\mathbb{C}$ is said to be a *number field*, if it is an extension of finite degree, $[k : \mathbb{Q}] = \dim_{\mathbb{Q}} k < \infty$. It follows automatically that $k \subset \overline{\mathbb{Q}} \subset \mathbb{C}$.

[15]For a variety X_k defined over a number field k, $X_k(L)$ for an extension L/k stands for the set of points where the coordinate values are in L.

[16]In the case $j = 1728$, E_{32A2} and E_{64A1} are examples of arithmetic models defined defined over $\mathbb{Q}$.

$$y^2 + xy = x^3 - \frac{36}{j(z) - 1728}x - \frac{1}{j(z) - 1728}$$

for $j(z) \neq 1728$ has the j-invariant equal to $j(z)$, so this is a model over $\mathbb{Q}(j(z))$. It is also known that, whenever $[E_z]_{\mathbb{C}}$ has a model over a number field k, there are infinitely many different models over k of $[E_z]_{\mathbb{C}}$. Those different models E_k have their own L-functions $L(E_k, s)$, which are defined similarly to the case of models defined over $k = \mathbb{Q}$ (the product over rational primes is replaced by the product over prime ideals of the ring of algebraic integers of the field k).

There are just 13 pairs (K, f_z) for which the set $\mathcal{E}ll(\mathcal{O}_{f_z})$ consists of just single element, and hence there are just 13 CM elliptic curves $[E_z]_{\mathbb{C}}$ defined over $\mathbb{C}$ that have $j(z) \in \mathbb{Q}$; the four among the 13 have already been presented explicitly in Example 2.1.1. For all other CM elliptic curves defined over $\mathbb{C}$, a model over $k = \mathbb{Q}$ is not available. For each one of the 13 CM elliptic curves $[E_z]_{\mathbb{C}}$ with $j(z) \in \mathbb{Q}$, there are infinitely many models defined over $\mathbb{Q}$; for the one with $j = 1728$, the two models E_{32A2} and E_{64A1} are only a small part of the models defined over $\mathbb{Q}$.

2.1.3. Elliptic curves of Shimura-type: classification and examples In the rest of this article, we will focus primarily on the cases with $f_z = 1$. We anticipate that the following theoretical development still holds true for cases with $f_z > 1$ after appropriate modifications, but we keep the story simple here by restricting our attention (some additional information may be found in [16], [17]). The ring $\mathcal{O}_{f_z}$ is denoted by $\mathcal{O}_K$, and the abelian group $\mathrm{Cl}_K(\mathcal{O}_{f_z=1})$ by Cl_K when $f_z = 1$.

We have stated a fact that there are only 13 CM elliptic curves defined over $\mathbb{C}$ that have arithmetic models over $\mathbb{Q}$; Deuring's theory [8] in combination of Eichler–Shimura theory work for all of their infinitely many arithmetic models. Shimura [26] formulated a broader class of arithmetic models of CM elliptic curves, which we call elliptic curves *of Shimura type* or arithmetic models *of Shimura type*, where the theory of Deuring–Eichler–Shimura can be generalized; we will explain in section 2.1.4 that a set of weight-2 cuspforms are associated with an elliptic curve of Shimura-type.

There are such arithmetic models of Shimura type, infinitely many in fact, for any one of CM elliptic curves defined over $\mathbb{C}$ with arbitrary (K, f_z), not just for the 13 of them with $h(\mathcal{O}_{f_z}) = 1$. Our goal in this article is to find a relation between the weight-2 modular forms associated with those arithmetic models of Shimura type and chiral correlation functions in string theory whose target space is $[E_z]_{\mathbb{C}}$.

More systematic and comprehensive expositions on the basic properties of elliptic curves of Shimura-type are given in the preprint version [17, §4.1.3]. There are two kinds of arithmetic models of Shimura-type; one is arithmetic models E defined over a number field k that is an abelian extension of K containing $H_K = L_{f_z=1}$, and the other is arithmetic models E' defined over a number field k that does not contain K but kK contains $H_K = L_{f_z=1}$. In this journal version of this article, we only refer to arithmetic models of the former kind;[17] a little more comments on the arithmetic models of the latter kind are also found in the preprint version [17].

Instead of giving a definition of the elliptic curves of Shimura type, let us state the result of classification of models of this class here. Fix an imaginary quadratic field $K = \mathbb{Q}(\sqrt{D_K})$ (and $f_z = 1$ already implicitly). For a given ideal[18] $\mathfrak{c}_f$ of the ring $\mathcal{O}_K$, one may list up all the characters χ'_f of the multiplicative group $[\mathcal{O}_K/\mathfrak{c}_f]^\times$ (the set of invertible elements of the ring $\mathcal{O}_K/\mathfrak{c}_f$ with respect to multiplication) that satisfies

$$\chi'_f(\omega + \mathfrak{c}_f) = \omega^{-1} \qquad {}^\forall\omega \in \mathcal{O}_K^\times. \tag{6}$$

For each χ'_f, it is known that each one of elliptic curves $[E_{z_a}]_\mathbb{C}$ over $\mathbb{C}$ in $\mathcal{E}ll(\mathcal{O}_K)$ (where $a = 1, \cdots, h(\mathcal{O}_K)$) has its arithmetic model of Shimura type E_{z_a}. That is a non-trivial statement, which we do not explain further here; we refer the reader to [16, §4.2] for the derivation.

The corresponding $h(\mathcal{O}_K)$ elliptic curves of Shimura type E_{z_a} all have the same field of definition k that is specified as follows. There must be a subgroup of $[\mathcal{O}_K/\mathfrak{c}_f]^\times$, denoted by $[\mathcal{O}_K/\mathfrak{c}_f]^\times_k$, where the values of the character χ'_f are within $\mathcal{O}_K^\times$. Because[19] any subgroup of $[\mathcal{O}_K/\mathfrak{c}_f]^\times$ determines a subgroup of the *ray ideal class group* $\mathrm{Cl}_K(\mathfrak{c}_f)$, an abelian extension k of K is determined by the condition that $\mathrm{Gal}(k/K) \cong \mathrm{Cl}_K(\mathfrak{c}_f)/[\mathcal{O}_K/\mathfrak{c}_f]^\times_k$; the number field k is contained in the *ray class field* $L_{\mathfrak{c}_f}$ (for more information, see [16, §4.2]).

[17]The arithmetic models E_{32A2} and E_{64A1} of $[E_{z=i}]_\mathbb{C}$ are of Shimura-type of the latter kind with $k = \mathbb{Q}$, but if we think of the coefficients in their defining equations as those in $K = \mathbb{Q}(\sqrt{-4}) = H_K$ (which just happen to be within $\mathbb{Q} \subset K$), then we are now seeing them as $E_{32A2} \otimes_\mathbb{Q} K$ and $E_{64A1} \otimes_\mathbb{Q} K$, of Shimura-type of the former kind with $k = K = H_K$.

[18]Only an ideal $\mathfrak{c}_f$ with the following property is considered: $x - 1 \notin \mathfrak{c}_f$ for any $x \in \mathcal{O}_K^\times \backslash \{1\}$.

[19]The global class field theory is being used here, but it is enough to keep in mind in order to follow the rest of the story that there is some widely accepted algorithm that determines a finite abelian extension k/K from the data at our disposal (i.e., the character χ'_f of the group $[\mathcal{O}_K/\mathfrak{c}_f]^\times$).

Example 2.1.2. Think of a case $K = \mathbb{Q}(\sqrt{-4})$, when the ring $\mathcal{O}_K$ is $\mathbb{Z}+\mathbb{Z}i$. When we choose the ideal $\mathfrak{c}_f$ to be $(4)_{\mathcal{O}_K} = 4\mathbb{Z}+4i\mathbb{Z} \subset \mathcal{O}_K$, then $[\mathcal{O}_K/\mathfrak{c}_f]^\times = \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/4\mathbb{Z}$, where we can choose the generator of $\mathbb{Z}/2\mathbb{Z}$ and $\mathbb{Z}/4\mathbb{Z}$ to be $3+2i+(4)_{\mathcal{O}_K}$ and $i+(4)_{\mathcal{O}_K}$, respectively.[20] This group has two characters χ'_f satisfying (6). One is $\chi'_{f;32A} : i \mapsto -i$ and $(3+2i) \mapsto 1$, and the other $\chi'_{f;64A} : i \mapsto -i$ and $(3+2i) \mapsto -1$. All the values of the characters $\chi'_{f;32A}$ and $\chi'_{f;64A}$ are in $\{\pm 1, \pm i\} = \mathcal{O}_K^\times$, so the subgroup $[\mathcal{O}_K/\mathfrak{c}_f]^\times_k$ is $[\mathcal{O}_K/\mathfrak{c}_f]^\times$ itself. For the elliptic curve $[E_{z=i}]_\mathbb{C}$ defined over $\mathbb{C}$ with $(K, f_z) = (\mathbb{Q}(\sqrt{-4}), 1)$, there are at least two elliptic curves of Shimura type corresponding to $\chi'_{f;32A}$ and $\chi'_{f;64A}$, whose field of definition k can be chosen as $H_K = K = \mathbb{Q}(\sqrt{-4}) = \mathbb{Q}(\sqrt{-1})$ itself.

It is known in fact that the two arithmetic models defined over K are actually $E_{32A2} \otimes_\mathbb{Q} K$ and $E_{64A1} \otimes_\mathbb{Q} K$, respectively.

Example 2.1.3. Think of a case $K = \mathbb{Q}(\sqrt{-8})$, where the ring $\mathcal{O}_K$ is $\mathbb{Z}+\mathbb{Z}\sqrt{2}i$. When we choose the ideal $\mathfrak{c}_f$ to be $(2\sqrt{2}i)_{\mathcal{O}_K} = 4\mathbb{Z}+2\sqrt{2}i\mathbb{Z}$, then $[\mathcal{O}_K/\mathfrak{c}_f]^\times \cong \mathbb{Z}/4\mathbb{Z}$ generated by $1+\sqrt{2}i+\mathfrak{c}_f$. There are two characters χ'_f of the group $[\mathcal{O}_K/\mathfrak{c}_f]^\times$ satisfying (6). So, for the CM elliptic curve $[E_{z=\sqrt{2}i}]_\mathbb{C}$ defined over $\mathbb{C}$ with $(K, f_z) = (\mathbb{Q}(\sqrt{-8}), 1)$, there are arithmetic models of Shimura type for those characters χ'_f (see below, however). The subgroup $[\mathcal{O}_K/\mathfrak{c}_f]^\times_k$ is $\mathbb{Z}/2\mathbb{Z} \subset \mathbb{Z}/4\mathbb{Z}$. So the field of definition k can be chosen as a degree-2 extension over $H_K = K = \mathbb{Q}(\sqrt{-8}) = \mathbb{Q}(\sqrt{-2})$ ramified over the prime ideal $(\sqrt{2}i)_{\mathcal{O}_K}$ of $\mathcal{O}_K$.

We note that the two characters agree, when they are restricted to the subgroup $[\mathcal{O}_K/\mathfrak{c}_f]^\times_k$ of $[\mathcal{O}_K/\mathfrak{c}_f]^\times$. This fact is used momentarily.

Example 2.1.4. Think of a case $K = \mathbb{Q}(\sqrt{-20})$, when the ring $\mathcal{O}_K$ is $\mathbb{Z} + \sqrt{5}i\mathbb{Z}$. When we choose the ideal $\mathfrak{c}_f$ to be $(2\sqrt{5}i)_{\mathcal{O}_K} = 10\mathbb{Z} + 2\sqrt{5}i\mathbb{Z}$, then $[\mathcal{O}_K/\mathfrak{c}_f]^\times \cong \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/4\mathbb{Z}$, where we can choose the generator of $\mathbb{Z}/2\mathbb{Z}$ and $\mathbb{Z}/4\mathbb{Z}$ to be $4+\sqrt{5}i+\mathfrak{c}_f$ and $3+\mathfrak{c}_f$, respectively. This multiplicative group has four characters satisfying (6); they are $\chi'_f(a,b) : (4+\sqrt{5}i+\mathfrak{c}_f) \mapsto (-1)^a$, $(3+\mathfrak{c}_f) \mapsto i^b$, with ${}^\forall a \in \{0,1\}$ and ${}^\forall b \in \{1,3\} \subset \{0,1,2,3\}$. So, for each of the CM elliptic curves $[E_{z_0}]_\mathbb{C}$ and $[E_{z_1}]_\mathbb{C}$ in (4) defined over $\mathbb{C}$, there exist four arithmetic models of Shimura type (see below, however). For all the four characters, the subgroup $[\mathcal{O}_K/\mathfrak{c}_f]^\times_k$ is $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z} \subset \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/4\mathbb{Z}$, so the field of definition k of the $h(\mathcal{O}_K) \times 4$ arithmetic models can be chosen as a degree-2 extension of $H_K = K(\sqrt{5}) = \mathbb{Q}(\sqrt{-5}, \sqrt{-1})$.

[20] $(3+2i+(4)_{\mathcal{O}_K})^2 = (3+2i)^2 + (4)_{\mathcal{O}_K} = 1 + (4)_{\mathcal{O}_K}$, so it is an element of order 2 in the group $[\mathcal{O}_K/(4)_{\mathcal{O}_K}]^\times$.

It is not hard to find out that the pair of characters $\chi'_f(0,1)$ and $\chi'_f(0,3)$ coincide on the subgroup $[\mathcal{O}_K/\mathfrak{c}_f]^\times_k$, and so do the pair $\chi'_f(1,1)$ and $\chi'_f(1,3)$. This fact is used below. •

We have quoted the result that enables us to list up all the elliptic curves of Shimura type, using the ideals $\mathfrak{c}_f$ and characters, but there are some redundancy among those models. There are two kinds of redundancy, in fact, so let us explain them in turn.

First, for a common ideal $\mathfrak{c}_f$, two characters $\chi'_{f(1)}$ and $\chi'_{f(2)}$ correspond to the same arithmetic model over k (i.e., there is an isomorphism defined over k between the two corresponding models) when the characters $\chi'_{f(1)}$ and $\chi'_{f(2)}$ of the group $[\mathcal{O}_K/\mathfrak{c}_f]^\times$ are identical when restricted upon the subgroup $[\mathcal{O}_K/\mathfrak{c}_f]^\times_k$. For example, it sounds as if Example 2.1.3 talks of two arithmetic models corresponding to two characters, in fact there is just one model defined over the degree-2 extension field k of H_K. Similarly, in Example 2.1.4, there are just $h(\mathcal{O}_K)\times 2$ arithmetic models modulo isomorphism over k, corresponding to the characters $\{\chi'_f(0,\pm1)\}$ and $\{\chi'_f(1,\pm1)\}$. To one k-isomorphism class of an elliptic curve of Shimura-type, E/k, with $[E]_\mathbb{C}\in \mathcal{E}ll(\mathcal{O}_K)$, correspond

$$\frac{\#[\mathcal{O}_K/\mathfrak{c}_f]^\times}{\#[\mathcal{O}_K/\mathfrak{c}_f]^\times_k} = \#\mathrm{Gal}(k/H_K)$$

distinct characters $\{\chi'_f\}$ of $[\mathcal{O}_K/\mathfrak{c}_f]^\times$.

Secondly, let the ideal $\mathfrak{c}_f$ vary. For two ideals $\mathfrak{c}_f$ and $\mathfrak{c}_{f'}$ of the ring $\mathcal{O}_K$, suppose that $\mathfrak{c}_f|\mathfrak{c}_{f'}$. Suppose further that a character $\chi'_{f'}$ of the group $[\mathcal{O}_K/\mathfrak{c}_{f'}]^\times$ is induced from a character χ'_f of $[\mathcal{O}_K/\mathfrak{c}_f]^\times$ through the projection $[\mathcal{O}_K/\mathfrak{c}_{f'}]^\times \to [\mathcal{O}_K/\mathfrak{c}_f]^\times$. Then the elliptic curve of Shimura type for χ'_f and $\chi'_{f'}$ are isomorphic over the field of definition k.

For example, in Example 2.1.2, the character $\chi'_{f;32A}$ we introduced for $\mathfrak{c}_f=(4)_{\mathcal{O}_K}$ can actually be induced from a character for $\mathfrak{c}_f=(2+2i)_{\mathcal{O}_K}$. Similarly, in Example 2.1.4, the characters $\{\chi'_f(1,\pm1)\}$ can be induced from a pair of characters for $\mathfrak{c}_f=(\sqrt{5}i)_{\mathcal{O}_K}$. The minimal choice of ideals $\mathfrak{c}_f$ of $\mathcal{O}_K$ for an arithmetic model E/k is called *the conductor*.

We have now quoted all the statements on the classification of elliptic curves of Shimura type. Despite the redundancy referred to above, for a given imaginary quadratic field K and $f_z=1$, each one $\mathbb{C}$-isomorphism class $[E_z]_\mathbb{C}$ of $\mathcal{E}ll(\mathcal{O}_K)$ has infinitely many distinct arithmetic models of Shimura type, with varying field of definition k that is an abelian extension of K.

2.1.4. Elliptic curves of Shimura-type: modular parametrization A theory of modular parametrization can be developed for all the elliptic curves of Shimura-type, similarly to the cases of arithmetic models of CM elliptic curves defined over $\mathbb{Q}$ (as illustrated by examples in section 1.1). Reference [28] wrote down such a theory of modular parametrization for the class of elliptic curves E' defined over a number field F that does not contain the imaginary quadratic field K; we referred to this class of arithmetic models as Shimura-type of latter kind early in section 2.1.3. We still need such a theory for arithmetic models of the former kind. So, the preprint version of this article [17, §4.1.3 and §4.1.4] did that task (almost parallel to [28]), by exploiting [12] and [21]. In this journal version, however, we just quote the results from there, which will be a sequence of highly non-trivial statements for large fraction of string theorists; readers with more familiarity in arithmetic geometry are referred to [17, §4.1.3 and §4.1.4].

Let E be an elliptic curve of Shimura type, defined over a number field k that is an abelian extension over K. An abelian variety B is defined by

$$B := \prod_{\sigma \in \mathrm{Gal}(k/K)} ({}^{\sigma}E),$$

which is of dimension $[k : K]$. It is known that the abelian variety B has an arithmetic model defined over the field K rather than k. In cases of CM elliptic curves E' defined over $\mathbb{Q}$, $E := E' \otimes_{\mathbb{Q}} K$ are of Shimura-type, with $k = K$, so the abelian variety B is nothing more than E.

It turns out that there is a map[21] from $\mathrm{Jac}(X_1(N)) \otimes_{\mathbb{Q}} K$ to B defined over K,

$$\nu : \mathrm{Jac}(X_1(N)) \otimes_{\mathbb{Q}} K \longrightarrow_{/K} B, \tag{7}$$

[21] As explained in textbooks, modular curves—the closure of the Riemann surfaces $\Gamma_0(N)\backslash\mathcal{H}$ and $\Gamma_1(N)\backslash\mathcal{H}$—have arithmetic models defined over $\mathbb{Q}$ (except for small number of N's which are irrelevant in the context of this article). From here on in this journal version of this article, $X_1(N)$ and $X_0(N)$ stand for such a model over $\mathbb{Q}$ (so, C and $X_0(64)$ in section 1.1 should be denoted by $X_0(64)$ and $X_0(64)\otimes\mathbb{C}$ now). We may sometimes use a notation $X_0(N)_{\mathbb{C}}$ and $X_1(N)_{\mathbb{C}}$ instead of $X_0(N)\otimes\mathbb{C}$ and $X_1(N)\otimes\mathbb{C}$.

When a curve C is defined over a number field, then its Jacobian variety is also defined over the same number field.

when we choose[22]

$$N \quad \text{divisible by } |D_K|\mathrm{Nm}_{K/\mathbb{Q}}(\mathfrak{c}_f). \tag{8}$$

By combining the Abel–Jacobi map $\mu : X_1(N) \to_{/\mathbb{Q}} \mathrm{Jac}(X_1(N))$ with this map, we also have a map $\nu' := (\nu \circ \mu) : X_1(N) \otimes_{\mathbb{Q}} K \to_{/K} B$.

In section 1.1, we illustrated by examples the theory of modular parameterization for arithmetic models over $\mathbb{Q}$ of CM elliptic curves. There, a surjective map $\nu' : X_0(64) \to E/\mathbb{Q}$ and $(\nu')^* : H^1([E]_{\mathbb{C}}, \mathbb{C}) \to H^1(X_0(64)_{\mathbb{C}}, \mathbb{C}) \cong H^1(\mathrm{Jac}(X_0(64))_{\mathbb{C}}, \mathbb{C})$ played a major role. Here, we have a surjective map $\nu : \mathrm{Jac}(X_1(N)) \otimes K \to_{/K} B/K$ instead; $H^1([E]_{\mathbb{C}}, \mathbb{C})$ is generalized to $H^1(B_{\mathbb{C}}, \mathbb{C})$, and $H^1(\mathrm{Jac}(X_0(64))_{\mathbb{C}}, \mathbb{C})$ to $H^1(\mathrm{Jac}(X_1(N))_{\mathbb{C}}, \mathbb{C})$.

Let us digress here for a moment to explain why the theory of modular parametrization is generalized in that way. It is an option for readers to skip this part until the end of this section 2.1.4 in the first reading, if the following materials are too much.

First, for an arithmetic model E defined over $\mathbb{Q}$, one may construct a representation of the Galois group $\mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})$, as follows. To start off, think of ℓ-power torsion points $E[\ell^n]$ for some prime integer $\ell \in \mathbb{N}$ and some $n \in \mathbb{N}$; they may be identified with automorphisms—translation by ℓ^n-torsion points in the fiber—of the covering $(\ell^n \times) : E \to E$. The collection of such automorphisms of the coverings with a fixed ℓ and varying n's form $\mathrm{Tate}_\ell(E/\mathbb{Q}) := \mathbb{Z}_\ell \oplus \mathbb{Z}_\ell := \varprojlim_{n\in\mathbb{N}} (\mathbb{Z}/\ell^n\mathbb{Z} + \mathbb{Z}/\ell^n\mathbb{Z})$. The coordinate values of those torsion points in E are algebraic numbers, so the Galois group acts on them; this is how we obtain $\rho_\ell(E/\mathbb{Q}) : \mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q}) \to M_{2\times 2}(\mathbb{Z}_\ell)$ represented on the space $\mathrm{Tate}_\ell(E/\mathbb{Q})$. The vector space $H^1_{et}(E\otimes\overline{\mathbb{Q}}, \overline{\mathbb{Q}}_\ell)$ is known to be the dual vector space of $\mathrm{Tate}_\ell(E/\mathbb{Q}) \otimes_{\mathbb{Z}_\ell} \overline{\mathbb{Q}}_\ell$, so we have a dual representation $\rho_\ell^\vee(E/\mathbb{Q})$ on this vector space; $\rho_\ell^\vee(E/\mathbb{Q})(\sigma) = [\rho_\ell(E/\mathbb{Q})(\sigma^{-1})]^T$ for $\sigma \in \mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})$. The L-function[23] $L(E/\mathbb{Q}, s)$ is defined by the product of the

[22] For an integral ideal $\mathfrak{q}$ of a ring $\mathcal{O}_L$ of all the algebraic integers in a number field L, $\mathrm{Nm}_{L/\mathbb{Q}}(\mathfrak{q}) := [\mathcal{O}_L : \mathfrak{q}]$.

[23] An easier example of L-functions is for a 1-dimensional Affine variety $\mathbb{G}_m := \{x \mid x \neq 0\}$. One may consider ℓ-power torsion points in $\mathbb{G}_m(\overline{\mathbb{Q}})$, $x = e^{2\pi i a/\ell^n} =: z_a$ with $a \in \mathbb{Z}/\ell^n\mathbb{Z}$; one may further see them as automorphisms $(z_a\times) : \mathbb{G}_m(\overline{\mathbb{Q}}) \ni x \mapsto z_a x \in \mathbb{G}_m(\overline{\mathbb{Q}})$ on the fibers of the ℓ^n-fold covering $\pi_{\ell^n} : \mathbb{G}_m(\overline{\mathbb{Q}}) \ni x \mapsto x^{\ell^n} \in \mathbb{G}_m(\overline{\mathbb{Q}})$. The collection of those automorphisms of the coverings forms $\mathbb{Z}_\ell = \varprojlim_{n\in\mathbb{N}} \mathbb{Z}/\ell^n\mathbb{Z}$, which is the prototype of the Tate module of an elliptic curve. The Galois group $\mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})$ acts on this set of fiber automorphisms as $(z_a\times) \mapsto \sigma_p \cdot (z_a\times) \cdot \sigma_p^{-1} =: (z_{a^{\sigma_p}}\times)$, where σ_p is the arithmetic Frobenius; to be more explicit, σ_p is a map

characteristic polynomials of $\rho_\ell^\vee(E/\mathbb{Q})(\sigma)$ labeled by a certain set $\{\sigma\}$ of elements—called Frobenii—of the group $\mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})$.

It is then easy to imagine that an abelian variety B defined over K [resp. an elliptic curve E of Shimura type defined over k], its Tate module $\mathrm{Tate}_\ell(B/K) \cong (\mathbb{Z}_\ell)^{\oplus 2[k:K]}$ and its dual space $H^1_{et}(B \otimes_K \overline{\mathbb{Q}}, \overline{\mathbb{Q}}_\ell)$ [resp. $\mathrm{Tate}_\ell(E/k) \cong (\mathbb{Z}_\ell)^{\oplus 2}$ and $H^1_{et}(E \otimes_k \overline{\mathbb{Q}}, \overline{\mathbb{Q}}_\ell)$] can be used to introduce the representations $\rho_\ell(B/K)$ and $\rho_\ell^\vee(B/K)$ [resp. $\rho_\ell(E/k)$ and $\rho_\ell^\vee(E/k)$] of the group $\mathrm{Gal}(\overline{\mathbb{Q}}/K)$ [resp. $\mathrm{Gal}(\overline{\mathbb{Q}}/k)$]. The representation $\rho_\ell^\vee(B/K)$ is the induced representation of $\rho_\ell^\vee(E/k)$ for the inclusion $\mathrm{Gal}(\overline{\mathbb{Q}}/k) \subset \mathrm{Gal}(\overline{\mathbb{Q}}/K)$, and the representation $\rho_\ell(B/K)$ that of $\rho_\ell(E/k)$.

The representation $\rho_\ell(B/K)$ of $\mathrm{Gal}(\overline{\mathbb{Q}}/K)$ would usually take values in $\overline{\mathbb{Q}}_\ell$-valued $2[k:K] \times 2[k:K]$ matrices. In the case E/k is an elliptic curve of Shimura type, however, the representation can be diagonalized in fact, and is split into $2[k:K]$ 1-dimensional $\overline{\mathbb{Q}}_\ell$-valued representations. This property is almost the defining property of elliptic curves of Shimura-type. The fact that there is a surjective map $\nu : \mathrm{Jac}(X_1(N)) \otimes K \to_{/K} B$ defined over K—a fact that we have already stated at (7)—implies that the representation space $H^1_{et}(B \otimes_K \overline{\mathbb{Q}}, \overline{\mathbb{Q}}_\ell)$ has a copy under the pull back in $H^1_{et}(\mathrm{Jac}(X_1(N)) \otimes \overline{\mathbb{Q}}, \overline{\mathbb{Q}}_\ell)$, so the latter vector space also supports $2[k:K]$ 1-dimensional representations of the group $\mathrm{Gal}(\overline{\mathbb{Q}}/K)$. Furthermore, $[k:K]$ of those 1-dimensional representations are generated by appropriate linear combinations of the holomorphic 1-forms[24] dx/y of

$$H^1(B \otimes \mathbb{C}, \mathbb{C}) \cong \oplus_{\sigma \in \mathrm{Gal}(k/K)} H^1({}^\sigma E \otimes \mathbb{C}, \mathbb{C}). \tag{9}$$

Those $[k:K]$ 1-forms are pulled back by ν^* to become the generators of the $[k:K]$ distinct 1-dimensional representations within $H^1_{et}(\mathrm{Jac}(X_1(N)) \otimes \overline{\mathbb{Q}}, \overline{\mathbb{Q}}_\ell)$.

We may think of the induced representations of the group $\mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})$ from the $2[k:K]$ representations of $\mathrm{Gal}(\overline{\mathbb{Q}}/K)$, but actually the $2[k:K]$ representations form $[k:K]$ pairs so that actually only $[k:K]$ distinct representations of $\mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})$ are constructed in this way (for more explanations,

---

$\sigma_p : \widetilde{\mathbb{G}_{mp}}(\overline{\mathbb{F}}_p) \ni x \mapsto (x)^{1/p} \in \widetilde{\mathbb{G}_{mp}}(\overline{\mathbb{F}}_p)$ on the reduction of $\mathbb{G}_m$ over the prime (p), denoted by $\widetilde{\mathbb{G}_{mp}}$. By fixing one identification between the ℓ^n-th roots of unity in $\overline{\mathbb{Q}}$ and those in $\overline{\mathbb{F}}_p$ (assuming $\ell \neq p$), we obtain $\mathbb{Z}/\ell^n\mathbb{Z} \ni a \mapsto a^{\sigma_p} = p' \cdot a \in \mathbb{Z}/\ell^n\mathbb{Z}$, where $pp' \equiv 1 \in \mathbb{Z}/\ell^n\mathbb{Z}$; in other words, $\rho_\ell(\mathbb{G}_m)(\sigma_p) = (p'\times)$. Under the dual representation, $\rho_\ell^\vee(\mathbb{G}_m)(\sigma_p) = (p\times)$. So, the L-function of the Galois representation on $H^1_{et}(\mathbb{G}_m \otimes \overline{\mathbb{Q}}, \overline{\mathbb{Q}}_\ell)$ is then $L(\mathbb{G}_m/\mathbb{Q}, s) := \prod_p [1 - \rho_\ell^\vee(\sigma_p) p^{-s}]^{-1} = \prod_p [1 - p \cdot p^{-s}]^{-1} = \zeta(s-1)$.

[24]We make use of $H^1_{et}(B \otimes_K \overline{\mathbb{Q}}, \overline{\mathbb{Q}}_\ell) \cong H^1(B \otimes \mathbb{C}, \mathbb{C})$ etc.

see [17, §4.1.4]). Those $[k : K]$ representations of $\mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})$ are therefore in one-to-one with the linear combinations of holomorphic 1-forms pulled back from the Galois conjugates of E/k; furthermore, those 1-forms are also regarded as elements of $H^1(X_1(N)_{\mathbb{C}}, \mathbb{C})$, or put differently,[25] as elements of weight-2 cusp forms of $\Gamma_1(N)$.

2.2. Physics preliminaries

Materials in section 2.2 are well-known to string theorists. They are only for the purpose of setting notations and also helping readers refresh memory without going through detailed calculations. See [18] and [13] for more information.

2.2.1. T^2-target rational $N = (2,2)$ SCFT Bosonic string theory with a T^2 target space becomes a rational CFT if and only if the target T^2 is regarded as a CM elliptic curve $[E_z]_{\mathbb{C}}$ under the complex structure in which the metric is Hermitian and constant (so, $[E_z]_{\mathbb{C}} \in \mathcal{E}ll(\mathcal{O}_{f_z})$ for some (K, f_z)), and the complexified Kähler parameter

$$\rho := \frac{1}{(2\pi)^2\alpha'}\left(\int_{T^2} B + i\int_{T^2} J\right)$$

takes value in the imaginary quadratic field K; here, B and J are the B-field and Kähler form, and α' the squared string length as in standard conventions in string theory. The CFT is diagonal if and only if there is a representative z' from the $\mathrm{SL}(2;\mathbb{Z})$ orbit of the complex structure parameter z so that

$$\rho = f_\rho z', \qquad {}^\exists f_\rho \in \mathbb{N}_{>0}. \tag{10}$$

So, for an elliptic curve with complex multiplication $[E_z]_{\mathbb{C}}$, its treatment in bosonic string theory can be a diagonal rational CFT in infinitely many different ways labeled by positive integers f_ρ. The same can be said about its treatment in Type II string theory.

In such a diagonal rational CFT, the holomorphic chiral algebra and the anti-holomorphic chiral algebra are isomorphic, by definition, and are given by the lattice vertex operator algebra of an even rank-2 positive definite lattice Λ, which is the kernel of the right-moving momenta

$$p_R : H^1(T^2;\mathbb{Z}) \oplus H_1(T^2;\mathbb{Z}) \cong \mathrm{II}_{2,2} \longrightarrow \mathbb{R}^2.$$

[25] Weight-2 cuspforms of a congruence subgroup Γ are regarded as holomorphic 1-forms on the corresponding modular curve $(X_\Gamma)_{\mathbb{C}}$, and vice versa. So, those two notions are treated interchangeably.

Its intersection form is given by the following matrix

$$f_\rho \begin{bmatrix} 2a_z & b_z \\ b_z & 2c_z \end{bmatrix};$$

the set of irreducible representations of the chiral algebra is

$$iReps = G_\Lambda := \Lambda^\vee/\Lambda, \qquad \#(iReps) = f_\rho^2 f_z^2 |D_K|.$$

The fusion algebra is the group ring $\mathbb{Z}[G_\Lambda]$ of the finite abelian group G_Λ.

2.2.2. The class of chiral correlation functions of interest In Type II string theory, with the target space being a CM elliptic curve $[E_z]_\mathbb{C}$ and the complexified Kähler parameter $\rho = f_z z$, one may think of the following class of observables:[26] for $\beta \in iReps$,

$$f^{\mathrm{II}}_{1\Omega'}(\tau_{ws};\beta) := \frac{-i}{2\pi}\sqrt{\frac{2}{\alpha'}}\mathrm{Tr}^{\mathrm{Rmnd}}_{V_\beta}\left[F e^{\pi i F} q_{ws}^{L_0-\frac{c}{24}}(\partial_u X^\mathbb{C})(u)\right]. \tag{11}$$

Here, we use a genus-1 worldsheet $\Sigma_{ws} = \{u \in \mathbb{C} \mid u \sim u+1,\ u \sim u+\tau_{ws}\}$, where $\tau_{ws} \in \mathcal{H}$ is the complex structure parameter of the $g=1$ worldsheet, and $q_{ws} := e^{2\pi i \tau_{ws}}$. A trace is taken over a Ramond-type irreducible representation $\beta \in iReps \cong \Lambda^\vee/\Lambda$ of the holomorphic chiral algebra. The operators L_0 and F are the zero modes of the holomorphic energy-momentum tensor and the holomorphic fermion number U(1) current, respectively. The operator $X^\mathbb{C}(u)$ is the chiral bosons corresponding to the complex coordinate of the target space $[E_z]_\mathbb{C}$

For later use in this article, let us write down well-understood facts that one can reproduce by simple computations. The complexified left-moving momentum[27] maps the U(1) charges in $\mathrm{II}_{2,2}$ as

$$\Omega' := \sqrt{\frac{\alpha'}{2}}p_L^\mathbb{C} : \mathrm{II}_{2,2} \longrightarrow \Omega'(\mathrm{II}_{2,2}) = -i\sqrt{\frac{2a_z f_\rho}{\#(G_\Lambda)}}\mathfrak{b}_z \subset \mathbb{C},$$

[26]Strictly speaking, string S-matrix elements are directly observable in physical processes, and the S-matrix elements are given by products of holomorphic chiral correlation functions like f^{II} here and anti-holomorphic ones integrated over the moduli space of the worldsheet ($\approx$ over τ_{ws}).

[27]The normalization convention is that $|\Omega'|^2/2$ is the partial contribution to the conformal weight.

where $\Omega'(\Lambda) = \sqrt{2a_z f_\rho}\mathfrak{b}_z \subset \mathbb{C}$. We will find it useful also to introduce a rescaled version of the map Ω':

$$\Omega := i\sqrt{\frac{\#(G_\Lambda)}{2a_z f_\rho}}\Omega',$$

when

$$\Lambda^\vee \cong \Omega(\mathrm{II}_{2,2}) = \mathfrak{b}_z, \qquad \Omega(\Lambda) = f_\rho f_z\sqrt{D_K}\mathfrak{b}_z. \tag{12}$$

The one-to-one correspondence between $iReps \cong \Lambda^\vee/\Lambda$ and the D0 Cardy states can be through

(13)
$$(f_\rho f_z\sqrt{D_K})^{-1}\times:\ iReps \cong \Omega(\mathrm{II}_{2,2})/\Omega(\Lambda) \longrightarrow (f_\rho f_z\sqrt{D_K})^{-1}\mathfrak{b}_z/\mathfrak{b}_z \subset [E_z]_\mathbb{C}.$$

The chiral correlation functions (11) can be easily computed.

$$f^{\mathrm{II}}_{1\Omega'}(\tau_{ws};\beta) = \vartheta^{1\Omega'}_\Lambda(\tau_{ws};\beta), \tag{14}$$

where

$$\vartheta^{1\omega}_L(\tau;x) := \sum_{y\in L, y+L=x} \omega(y)e^{2\pi i\tau\frac{\langle y,y\rangle_L}{2}}$$

for an even lattice L, $x \in L^\vee/L$, $\tau \in \mathcal{H}$, and a linear map $\omega : L^\vee \to \mathbb{C}$. In the case of T^2-target string theory, the correlation functions $f^{\mathrm{II}}_{1\Omega'}$ have contributions from Kaluza–Klein and winding states on worldsheet, while stringy oscillator excitations cancel due to the $e^{\pi i F}F$ insertions.

3. Main ideas and the easiest example

Choose a target space of Type II string by fixing the data $([E_z]_\mathbb{C}, f_\rho)$; in the rest of this article, $[E_z]_\mathbb{C}$ always stands for a CM elliptic curve modulo isomorphisms over $\mathbb{C}$ and $f_\rho \in \mathbb{N}_{>0}$ for the parameter in (10) effectively governing the complexified Kähler parameter ρ. The set of chiral correlation functions $\{f^{\mathrm{II}}_{1\Omega'}(\beta)\}_{\beta\in iReps}$ forms a vector-valued modular form of weight-2 for the group $\mathrm{SL}(2;\mathbb{Z})_{ws}$, which acts on the complex structure parameter τ_{ws} of worldsheet through the ordinary linear fractional transformation. The characters (without the $F\partial X^\mathbb{C}$ insertion) are of weight-0 and are under the Weil representation of $\mathrm{SL}(2;\mathbb{Z})_{ws}$ associated with the lattice Λ, and $\{f^{\mathrm{II}}_{1\Omega'}\}$ is under the same representation, but of a different weight because of the insertions $F\partial X^\mathbb{C}$.

3.1. Observation 1: lift to modular curves

The kernel of the Weil representation of $\mathrm{SL}(2;\mathbb{Z})$ contains a principal congruence subgroup $\Gamma(N_{D\Lambda})$ [27],[28] where $N_{D\Lambda}$ is the *level*[29] of the quadratic discriminant form (G_Λ, q_Λ) of the lattice Λ; the formula for the level $N_{D\Lambda}$ in the cases of our interest (where Λ is an even positive definite rank-2 lattice) is found in (15). This means that individual $f^{\mathrm{II}}_{1\Omega'}(\tau_{ws}, \beta)$'s are regarded as scalar-valued weight-2 cuspforms for $\Gamma(N_{D\Lambda}) \subset \mathrm{SL}(2;\mathbb{Z})_{ws}$. Equivalently, $d\tau_{ws} f^{\mathrm{II}}_{1\Omega'}(\tau_{ws}, \beta)$ for each $\beta \in iReps$ is a holomorphic 1-form well-defined over the modular curve $X(N_{D\Lambda})_{\mathbb{C}}$, the closure of the Riemann surface $\Gamma(N_{D\Lambda})\backslash\mathcal{H}$.

The level $N_{D\Lambda}$ of the discriminant form is[30]

$$N_{D\Lambda} = f_\rho f_z^2 |D_K| \tag{15}$$

when the target space is $([E_z]_{\mathbb{C}}, f_\rho)$; a proof is elementary, and is found in the preprint version [17, Lemma 2.4.3]. Note that this level $N_{D\Lambda}$, and hence the modular curve $X(N_{D\Lambda})_{\mathbb{C}}$ depends only on $\mathcal{E}ll(\mathcal{O}_{f_z})$ and f_ρ, common to all of $h(\mathcal{O}_{f_z})$ isomorphism classes $[E_z]_{\mathbb{C}}$ in $\mathcal{E}ll(\mathcal{O}_{f_z})$.

For any $N \in \mathbb{N}_{>0}$, there is a natural inclusion

$$\pi_N^* : S_2(\Gamma(N)) \ni f(\tau) \longmapsto \pi_N^*(f)(\tau) := f(N\tau) \in S_2(\Gamma_1(N^2)),$$

which is the pull-back of 1-forms by the projection map

$$\pi_N : X_1(N^2)_{\mathbb{C}} \longrightarrow X(N)_{\mathbb{C}}.$$

For string theorists, it will be most natural to think of the chiral correlation functions $\{f^{\mathrm{II}}_{1\Omega'}(\tau_{ws};\beta)\}_{\beta\in iReps}$ either as a vector-valued local section on $\mathrm{PSL}(2;\mathbb{Z})_{ws}\backslash\mathcal{H}$, or a set of scalar-valued functions on $\mathcal{H}$; as a reminder, $\tau_{ws} \in \mathcal{H}$. It is not the first idea to come up with to lift the $g = 1$ chiral correlation functions only partially to the modular curves $\Gamma(N_{D\Lambda})\backslash\mathcal{H}$ or $\Gamma_1(N_{D\Lambda}^2)\backslash\mathcal{H}$ from $\mathrm{PSL}(2;\mathbb{Z})_{ws}\backslash\mathcal{H}$, not all the way to $\mathcal{H}$. Motivations to deal with the chiral correlation functions $f^{\mathrm{II}}_{1\Omega'}(\tau_{ws};\beta)$ as objects on modular curves entirely come from the side of arithmetic geometry.

[28] Additional explanations in [17, §2.4] and references therein may also provide useful information.

[29] For a finite quadratic form (G, q) with the convention that q is $\mathbb{Q}/2\mathbb{Z}$-valued, its *level* is the GCD of integers N such that $Nq(x) = 0 \in \mathbb{Q}/2\mathbb{Z}$ for all $x \in G$.

[30] This (15) holds true for any $f_z \in \mathbb{N}_{>0}$, although we will focus on the $f_z = 1$ cases in this journal version.

From the perspective of arithmetic geometry, there is a clear difference between $\mathcal{H}$ and the modular curves $(X_\Gamma)_{\mathbb{C}} = \overline{\Gamma\backslash\mathcal{H}}$. One is the fact [9, §7.6] that the modular curves $(X_\Gamma)_{\mathbb{C}}$ can be regarded as closed algebraic varieties, and moreover, have arithmetic models X_Γ defined over number fields $k_{\rm mod} \subset \overline{\mathbb{Q}}$; we have already illustrated this in section 1.1, where $X_0(64)$ was regarded as a variety with a model defined over $k_{\rm mod} = \mathbb{Q}$. One may then think of action of the Galois group $\mathrm{Gal}(\overline{\mathbb{Q}}/k_{\rm mod})$ on function fields and cohomology groups of X_Γ. On the other hand, $\mathcal{H}$ as a whole does not have that property.

The other difference is that the space of all the modular forms of a fixed weight (for some congruence subgroup ${}^\exists\Gamma \subset \mathrm{SL}(2;\mathbb{Z})$) is horribly complicated. On the other hand, the vector space of modular forms for a given congruence subgroup Γ forms a finite dimensional vector space, and moreover, one can derive a lot more knowledge on the substructure in this finite dimensional vector space (see such textbooks as [9] and [19], or a review in the appendix A.1 for a shortcut) by exploiting the action of the Hecke algebra.

As one can easily imagine, the chiral correlation functions $f^{\rm II}_{1\Omega'}(\tau_{ws};\beta)$ can be regarded as 1-forms not just on the curves $X(N_{D\Lambda})_{\mathbb{C}}$ and $X_1(N^2_{D\Lambda})_{\mathbb{C}}$, but also on any one of the curves $X(M)_{\mathbb{C}}$ and $X_1(M')_{\mathbb{C}}$ such that $N_{D\Lambda}|M$ and $N^2_{D\Lambda}|M'$. There must be some identification among the 1-forms[31] on those modular curves, and the direct limit is the right language to deal with this identification; the level M (and M') plays the role of the directed partially ordered set, with the ordering with respect to divisibility among them. The same argument can be made from the perspective of arithmetic geometry. The use of inverse/direct limit becomes all the more vital, when we discuss the effect of freedom in the choice of the target space parameter f_ρ in string theory; see Observation 4 in section 4.3.

It is one of central questions in this article how general the relation between the CFT correlation functions and the arithmetic modular forms is. Here is an observation that makes us feel that the relation is not just outright coincidence. As we have illustrated / explained in sections 1.1 and 2.1.4, the weight-2 modular forms f that are associated with the L-functions of the Galois representations of the arithmetic models are obtained as pullbacks of the 1-forms of the target space E/k by the map $\nu \circ \mu : X_\Gamma \to E$.

[31] Relevant discussion in the preprint version [17, §3.5] says a little more on a variety of ways to identify them.

The upper-right edge of the triangle diagram below refers to that fact:

(16)
$$\begin{tikzcd}
f^{\mathrm{II}}_{1\Omega'}(\tau_{ws};\beta) \in S_2(\Gamma) & X_0(N) \text{ or } X_\Gamma \arrow[ddr, "\nu\circ\mu"] & d\tau f(\tau) = \\
\propto \mathrm{Tr}[q^{L_0-c/24}e^{\pi i F}F\phi^*(\omega_E)]. & & (\nu\circ\mu)^*(\omega_E). \\
Map(\Sigma_{ws},([E]_{\mathbb{C}},f_\rho)) \ni \phi : \Sigma_{ws} \arrow[u, dotted, dash] \arrow[rr] & & E/\mathbb{Q} \text{ or } E/k
\end{tikzcd}$$

The chiral correlation functions $f^{\mathrm{II}}_{1\Omega'}$ of our interest are the sum of the operator $du(\partial_u X^{\mathbb{C}})$ matrix elements weighted by the factor $q^{L_0-c/24}e^{\pi i F}F$. This $dX^{\mathbb{C}}$ is the holomorphic (1,0)-form of the target space $[E]_{\mathbb{C}}$, so it is ω_E. The $N=(2,2)$ SCFT in consideration is formulated (roughly speaking) by using path-integration over the space $Map(\Sigma_{ws},([E]_{\mathbb{C}},f_\rho))$, and the operator $(du\partial_u X^{\mathbb{C}})$ is equivalent to

$$P^{(1,0)}\left(\phi^*(dX^{\mathbb{C}})\right) \propto P^{(1,0)}\left(\phi^*(\omega_E)\right); \tag{17}$$

here, $P^{(1,0)}$ is the projection $H^1(\Sigma_{ws};\mathbb{C}) \to H^{1,0}(\Sigma_{ws};\mathbb{C})$, and ϕ is the map from the worldsheet Σ_{ws} to the target space $([E]_{\mathbb{C}},f_\rho))$. Now, we lift the correlation functions $f^{\mathrm{II}}_{1\Omega'}(\beta)$ to 1-forms on the modular curve $X_1(N^2_{D\Lambda})$ (the upper left edge of the triangle diagram above). We have two ways to obtain 1-forms on the modular curves; one is to pull-back ω_E on the target space E/k by maps $X_\Gamma \to E/k$ in the theory of modular parametrization, and the other is to pull-back $\omega_E \propto dX^{\mathbb{C}}$ by the path-integral in string theory. Both the arithmetic modular forms for the Galois representations and the chiral correlation functions $f^{\mathrm{II}}_{1\Omega'}$ are obtained as a consequence of probing the same thing (1-form on the elliptic curves), by using maps in those two different theoretical framework. The relations between them may not be just a sheer coincidence, but may have a bit of substance.

3.2. Observation 2: the CM group

The chiral correlation functions $f^{\mathrm{II}}_{1\Omega'}(\tau_{ws};\beta)$ are now regarded as 1-forms on $X(N_{D\Lambda})_{\mathbb{C}}$. They generate a vector space of 1-forms $F([z],f_\rho)$ within

$S_2(\Gamma(N_{D\Lambda})) \cong H^{1,0}(X(N_{D\Lambda})_{\mathbb{C}};\mathbb{C})$; they are not linearly independent within $F([z], f_\rho)$, in fact; furthermore, one could think of choosing a basis of the vector space $F([z], f_\rho)$ from $\{f^{\rm II}_{1\Omega'}(\beta)\}_{\beta\in iReps}$, which one may call a VOA basis, but there may be other choices of basis of $F([z], f_\rho)$ that is more suitable for certain purposes. That is indeed the case in the context of the theory of modular parametrization for CM elliptic curves, as we see in the following. So, we introduce an idea that is also natural in rational CFT that leads to another choice of basis of the vector space $F([z], f_\rho)$.

Let us begin with the following observation. Given the identification (13), any complex multiplication $\alpha \in \mathcal{O}_{f_z}$ of $[E_z]_{\mathbb{C}}$ induces a map from $iReps \subset [E_z]_{\mathbb{C}}$ to itself. Now, we define a subset of $\mathcal{O}_{f_z}$,

$$\begin{aligned}\underline{\mathfrak{c}}([E_z]_{\mathbb{C}}, f_\rho) &:= \{\alpha \in \mathcal{O}_{f_z} \mid (1+\alpha) = \mathrm{id} : iReps \to iReps\} \\ &= \left\{\alpha \in \mathcal{O}_{f_z} \mid \alpha\Omega'(\Lambda^\vee) \subset \Omega'(\Lambda)\right\},\end{aligned}$$

which is an integral ideal of $\mathcal{O}_{f_z}$. Two complex multiplications $\alpha_1, \alpha_2 \in \mathcal{O}_{f_z}$ induce an identical map from $iReps \subset [E_z]_{\mathbb{C}}$ to itself, if and only if $\alpha_1 - \alpha_2$ is in the ideal $\underline{\mathfrak{c}}$. So, a map from $iReps$ to itself is defined for individual elements of $\mathcal{O}_{f_z}/\underline{\mathfrak{c}}$. Such a map $iReps \to iReps$ is not necessarily injective or surjective for an arbitrary element of the ring $[\mathcal{O}_{f_z}/\underline{\mathfrak{c}}]$. For an element in $[\mathcal{O}_{f_z}/\underline{\mathfrak{c}}]^\times$, however, there is an inverse in the multiplication law of $\mathcal{O}_{f_z}/\underline{\mathfrak{c}}$, and forms a multiplicative group. We call this finite abelian group *the CM group of the rational CFT* for $([E_z], f_\rho)$.

One can verify through calculations faithful to the definition above that

$$\underline{\mathfrak{c}} = \left(f_\rho f_z \sqrt{D_K}\right)_{\mathcal{O}_{f_z}}. \tag{18}$$

Readers might refer to the preprint version [17, §3.1.1] for a little more information on the proof of this statement. It follows immediately that the CM group is identical for all the rational CFTs corresponding to the set of target spaces $([E_z]_{\mathbb{C}}, f_\rho)$ with a common f_ρ, K and f_z but with different $[E_z]_{\mathbb{C}}$'s in a common $\mathcal{E}ll(\mathcal{O}_{f_z})$. We will use this fact in section 4.2 (and also implicitly in sections 4.1 and 4.3).

The CM group $[\mathcal{O}_{f_z}/\underline{\mathfrak{c}}]^\times$ contains the automorphism group $\mathcal{O}^\times_{f_z}$ of the target space $[E_z]_{\mathbb{C}}$. Each one of elements of the CM group induces an automorphism of the fusion algebra $\mathbb{Z}[iReps]$, and hence the CM group is contained[32] in $\mathrm{Aut}(\mathbb{Z}[iReps])$ as a subgroup.[33]

Now, let us discuss choices of basis of the vector space $F([z], f_\rho)$ once again. Let $G^*_\Lambda \subset G_\Lambda$ be where $f^{\mathrm{II}}_{1\Omega'}(\beta)$ is not trivially zero; β's in G^*_Λ forming an orbit of the automorphism group $\mathcal{O}^\times_{f_z} = \mathrm{Aut}([E_z]_\mathbb{C}) =: G_0$ of the target space give rise to just one linear independent one, $f^{\mathrm{II}}_{1\Omega'}(\tau_{ws}; g_0^{-1} \cdot \beta) = f^{\mathrm{II}}_{1\Omega'}(\tau_{ws}; \beta)(\rho^1)^{-1}(g_0)$, ${}^\forall g_0 \in \mathcal{O}^\times_{f_z}$, where ρ^1 is the embedding $K \to \mathbb{C}$ that maps $\sqrt{D_K}$ into the upper complex half plane. On the vector space

$$F([z], f_\rho) = \mathrm{Span}_\mathbb{C} \left\{ f^{\mathrm{II}}_{1\Omega'}(\tau_{ws}; \beta_0) \mid \text{choose a repr}'\text{tive } \beta_0 \in [\beta],\ {}^\forall[\beta] \in G^*_\Lambda / G_0 \right\}, \tag{19}$$

one may now think of the CM group $G \cong [\mathcal{O}_{f_z}/\underline{\mathfrak{c}}]^\times$ action where the VOA basis elements above are mapped by $g \in G$ as $f^{\mathrm{II}}_{1\Omega'}(\beta) \longmapsto f^{\mathrm{II}}_{1\Omega'}(g^{-1} \cdot \beta)$. Then it makes sense to reorganize the chiral correlation functions under the action of the subgroup G of the automorphism groups of the fusion algebra; this is indeed sensible thing to do from the perspective of arithmetic geometry (as we explain at the beginning of the preprint version [17, §3.1]). Because the CM group $[\mathcal{O}_{f_z}/\underline{\mathfrak{c}}]^\times$ is abelian, the representation space $F([z], f_\rho)$ can be decomposed into subspaces

$$F([z], f_\rho) \cong \oplus_{\chi_f^{-1} \in \mathrm{Char}([\mathcal{O}_{f_z}/\underline{\mathfrak{c}}]^\times)} F([z], f_\rho)^{\chi_f^{-1}} \tag{20}$$

where each subspace is the representation space (allowing multiplicity larger than 1) of a character χ_f^{-1} of the group $[\mathcal{O}_{f_z}/\underline{\mathfrak{c}}]^\times$.

[32] The fusion algebra here is the group algebra $\mathbb{Z}[iReps]$ of $iReps$ over $\mathbb{Z}$ where $iReps \cong \Lambda^\vee/\Lambda$ is an abelian group. We know (cf. [25, p.198, Prop 36.1]) that the automorphism group of the fusion algebra is isomorphic to the automorphism group of the abelian group $iReps$. Thus, the CM group can be regarded as a subgroup of the automorphism group of the fusion algebra. It is in general merely a proper subgroup; not all automorphisms of the fusion algebra can be regarded as elements of the CM group.

[33] Reference [10] identifies a subgroup of $\mathrm{Aut}(\mathbb{Z}[iReps])$ of a model of rational CFT in the following way. The Galois action on the monodromy representation matrices ([5], [3]) induces permutation on $iReps$ where $0 \in iReps$ (the vacuum repr) is mapped to itself. Such a Galois action is a symmetry of the fusion algebra and the charge conjugation combined [10]. The authors of the present article are not ready to state the relation between this subgroup of $\mathrm{Aut}(\mathbb{Z}[iReps])$ and the CM group in the case of T^2-target models.

The vector space $F([z], f_\rho)^{\chi_f^{-1}}$ is generated by the linear combinations of the chiral correlation functions of the form

(21)

$$f^{\rm II}_{1\Omega'}(\tau_{ws}; [\beta_0]; \chi_f) := \frac{1}{\#(\mathrm{Aut}([E_z]_{\mathbb{C}}))\#([\mathcal{O}_{f_z}/\underline{\mathfrak{c}}]^\times_{\beta_0})} \sum_{g' \in [\mathcal{O}_{f_z}/\underline{\mathfrak{c}}]^\times} \chi_f(g')\, f^{\rm II}_{1\Omega'}(\tau_{ws}; (g')^{-1}\cdot\beta_0)$$

for the CM group orbits $[\beta_0]$'s (where an orbit $[\beta_0]$ is represented by β_0 in G^*_Λ); here, $[\mathcal{O}_{f_z}/\underline{\mathfrak{c}}]^\times_{\beta_0}$ is the isotropy subgroup of the CM group at $\beta_0 \in iReps$. To see this, one just has to note that

$$\begin{aligned} g \cdot f^{\rm II}_{1\Omega'}([\beta_0]; \chi_f) &= \frac{1}{\#(\mathrm{Aut}([E_z]_{\mathbb{C}}))\#([\mathcal{O}_{f_z}/\underline{\mathfrak{c}}]^\times_{\beta_0})} \sum_{g' \in [\mathcal{O}_{f_z}/\underline{\mathfrak{c}}]^\times} \chi_f(g')\, f^{\rm II}_{1\Omega'}(g^{-1}\cdot(g')^{-1}\cdot\beta_0) \\ &= \frac{\chi_f^{-1}(g)}{\#(\mathrm{Aut}([E_z]_{\mathbb{C}}))\#([\mathcal{O}_{f_z}/\underline{\mathfrak{c}}]^\times_{\beta_0})} \sum_{g' \in [\mathcal{O}_{f_z}/\underline{\mathfrak{c}}]^\times} \chi_f(g'g)\, f^{\rm II}_{1\Omega'}(g^{-1}\cdot(g')^{-1}\cdot\beta_0) \\ &= \chi_f^{-1}(g)\, f^{\rm II}_{1\Omega'}([\beta_0]; \chi_f). \end{aligned}$$

The action of $g \in [\mathcal{O}_{f_z}/\underline{\mathfrak{c}}]^\times$ on $f^{\rm II}_{1\Omega'}$'s is the one introduced just below (19).

3.3. The example $[E_z]_{\mathbb{C}}$ with $z = i$: $j = 1728$

Take an example of a CM elliptic curve $[E_z]_{\mathbb{C}}$ with $z = i$, the elliptic curve with the j-invariant $j(z) = 1728$; as a reminder, $K = \mathbb{Q}(\sqrt{-1})$, $\mathcal{O}_K = \mathbb{Z}[i]$, $D_K = -4$, and $h(\mathcal{O}_K) = 1$ then. Now,

$$G_\Lambda \cong \mathbb{Z}/2f_\rho\mathbb{Z} \oplus \mathbb{Z}/2f_\rho\mathbb{Z}, \qquad N_{D\Lambda} = |D_K| f_z^2 f_\rho = 4f_\rho. \tag{22}$$

In the rational SCFT corresponding to the target space $([z], f_\rho) = ([i], 1)$, i.e., $f_\rho = 1$, $G_{\Lambda_-} \cong \mathbb{Z}/2\mathbb{Z} \oplus \mathbb{Z}/2\mathbb{Z}$ consists only of 2-torsion elements, and the chiral correlation function $f^{\rm II}_{1\Omega'}(\tau_{ws}; \beta)$ vanishes for any one of $\beta \in G_\Lambda$. This observation fits very well with the fact that the kernel of $\rho^{\rm Weil}_{D\Lambda}$ for $f_\rho = 1$ contains $\Gamma(4f_\rho) = \Gamma(4)$, and the vector space $S_2(\Gamma(4))$ is known to be empty.

In the rational SCFT corresponding to the target space $([z], f_\rho) = ([i], 2)$, the vector space $F([i], 2)$ of the chiral correlation functions $f^{\rm II}_{1\Omega'}$'s is of 3-dimensions over $\mathbb{C}$. One way to see it is to write down their CM-group-diagonal linear combinations (21) explicitly and check their linearly independence. To be more explicit, note first that the CM group in this case is

$[\mathcal{O}_K/\underline{\mathfrak{c}}]^\times = [\mathcal{O}_K/(4)_{\mathcal{O}_K}]^\times \cong \mathbb{Z}/2\mathbb{Z}\times\mathbb{Z}/4\mathbb{Z}$, where the first factor is generated by an order-2 element $(3+2i)+\underline{\mathfrak{c}}$, and the second factor by an order-4 element $i+\underline{\mathfrak{c}}$; the $\mathrm{Aut}([E_z]_{\mathbb{C}}) \cong \mathbb{Z}/4\mathbb{Z}$ subgroup of the CM group $[\mathcal{O}_K/\underline{\mathfrak{c}}]^\times$ is precisely the second factor $\mathbb{Z}/4\mathbb{Z}$ generated by $[(i)\times]$, the multiplication of i.

We know that the CM group $[\mathcal{O}_K/\underline{\mathfrak{c}}]^\times$ acts on the vector space $F([z], f_\rho)$ so that the restriction of the characters χ_f^{-1} on $\mathrm{Aut}([E_z]_{\mathbb{C}}) \subset [\mathcal{O}_K/\underline{\mathfrak{c}}]^\times$ is $(\rho^1)^{-1}$ (see just above (19)). So, there are two such characters;[34] for $a \in \mathbb{Z}/2\mathbb{Z}$, $\chi_f(a,1) : [(3+2i)\times] \mapsto (-1)^a$ and $[i\times] \mapsto i$.

The set G^*_Λ consists of $4^2 - 2^2 = 12$ elements, and is decomposed into two orbits of the CM group:

$$\mathrm{orb}_{\mathfrak{q}=\mathcal{O}_K} = \{1, i, 3, 3i, 3+2i, 2+3i, 1+2i, 2+i\}, \tag{23}$$
$$\mathrm{orb}_{\mathfrak{q}=(1+i)} = \{1+i, 3+i, 3+3i, 1+3i\}. \tag{24}$$

The irreducible representations, β's in $\Lambda^\vee/\Lambda \cong G_\Lambda$, are referred to above by the complex value (mod $\Omega(\Lambda)$) of their linear map Ω; we will use the same convention in expressing the argument β in $f^{\mathrm{II}}_{1\Omega'}$ and $\vartheta^{1\Omega}_\Lambda$ in the following.

Now it is straightforward to compute the combinations (21) explicitly, by using what we know about the chiral correlation functions, that is, (14).

$$\begin{aligned}
\frac{f_\rho f_z\sqrt{D_K}}{\sqrt{2f_\rho}}\, & f^{\mathrm{II}}_{1\Omega'}([1], \chi_f(1,1)) \\
&= \frac{f_\rho f_z\sqrt{D_K}}{\sqrt{2f_\rho}} \left(f^{\mathrm{II}}_{1\Omega'}(\tau_{ws}; 1) - f^{\mathrm{II}}_{1\Omega'}(\tau_{ws}; 3+2i)\right), \\
&= \sqrt{a_z}\left(\vartheta^{1\Omega}_\Lambda(\tau_{ws}, 1) - \vartheta^{1\Omega}_\Lambda(\tau_{ws}, 3+2i)\right), \\
&= (q - 3q^9 + 2q^{17} + \cdots) + 2(q^5 - q^{13} + \cdots),
\end{aligned} \tag{25}$$

$$\begin{aligned}
\frac{f_\rho f_z\sqrt{D_K}}{\sqrt{2f_\rho}}\, & f^{\mathrm{II}}_{1\Omega'}([1], \chi_f(0,1)) \\
&= \frac{f_\rho f_z\sqrt{D_K}}{\sqrt{2f_\rho}} \left(f^{\mathrm{II}}_{1\Omega'}(\tau_{ws}; 1) + f^{\mathrm{II}}_{1\Omega'}(\tau_{ws}; 3+2i)\right), \\
&= \sqrt{a_z}\left(\vartheta^{1\Omega}_\Lambda(\tau_{ws}, 1) + \vartheta^{1\Omega}_\Lambda(\tau_{ws}, 3+2i)\right), \\
&= (q - 3q^9 + 2q^{17} + \cdots) - 2(q^5 - q^{13} + \cdots),
\end{aligned} \tag{26}$$

$$\frac{f_\rho f_z\sqrt{D_K}}{\sqrt{2f_\rho}}\, f^{\mathrm{II}}_{1\Omega'}([1+i], \chi_f(1,1)) = 0, \tag{27}$$

[34]The conductor is $\mathfrak{c}_f = (4)_{\mathcal{O}_K}$ if $a = 1 \in \mathbb{Z}/2\mathbb{Z}$, and $\mathfrak{c}_f = (2+2i)_{\mathcal{O}_K}$ if $a = 0 \in \mathbb{Z}/2\mathbb{Z}$.

$$\begin{aligned}(28)\qquad \frac{f_\rho f_z\sqrt{D_K}}{\sqrt{2f_\rho}}\, & f^{\rm II}_{1\Omega'}([1+i],\chi_f(0,1)) \\ &= \frac{f_\rho f_z\sqrt{D_K}}{\sqrt{2f_\rho}} f^{\rm II}_{1\Omega'}(1+i) \\ &= (1+i)\left(q^2-2q^{10}-3q^{18}+\cdots\right);\end{aligned}$$

we have used $q := e^{2\pi i\tau}$ and $\tau_{ws} =: N_{D\Lambda}\tau$. Obviously they are linearly independent over $\mathbb{C}$, and hence $F([i],2)$ is of 3-dimensions indeed.

As we have explained already in section 3.1, those chiral correlation functions must be weight-2 modular forms for $\Gamma(N_{D\Lambda})$ when we see them as functions of τ_{ws}, and be those for $\Gamma_1(N_{D\Lambda}^2)$ when we see them as functions of τ. In the present case of the rational SCFT for the target space $([z],f_\rho)=([i],2)$, $N_{D\Lambda}=8$. The three linear combinations (25, 26, 28) indeed correspond/are proportional to X_1+X_5, X_1-X_5 and X_2 in section 1.1 that generate the 3-dimensional vector space $S_2(\Gamma_0(64))\subset S_2(\Gamma_1(64))$ of weight-2 cuspforms for $\Gamma_0(64)$.

The specific choice (25, 26, 28) as a basis of the 3-dimensional vector space $F([i],2)$ was motivated in section 3.2 as the diagonalization basis of the action of the CM group. This is also a good choice of a basis from the perspective of arithmetic geometry, although we do not explain in this journal version (found in the preprint version [17, §3.1]). One may still find it reasonable to accept that that is so, by noting that the combination (25) of the chiral correlation functions agrees with the modular form f_{64A1} of the arithmetic model E_{64A1} of the target space $[E_{z=i}]_{\mathbb{C}}$, and the combination (26) with the modular form f_{32A2} of the arithmetic model E_{32A2} of the same target space; see (2, 1). One will also find that the remaining combination (28) of the chiral correlation functions of the rational SCFT for $([z],f_\rho)=([i],2)$ is proportional to f_{32A2}=(26) with τ replaced by 2τ; this is called an *oldform* of f_{32A2} in the jargon of modular forms.

For the two arithmetic models $E_{32A2}\otimes K$ and $E_{64A1}\otimes K$ of $[E_{z=i}]_{\mathbb{C}}$, their modular forms f_{32A2} and f_{64A1} are expected—in the theory of modular parametrization—to be regarded as objects in $S_2(\Gamma_1(M))$ with $64|M$; this is because their conductors[35] $\mathfrak{c}_f=(2+2i)_{\mathcal{O}_K}$ and $(4)_{\mathcal{O}_K}$ divide indicate the levels divisible by $|D_K|\mathrm{Nm}_{K/\mathbb{Q}}((4)_{\mathcal{O}_K})=4\times 4^2=64$ (see the condition (8)). In the language of string theory, on the other hand, the chiral correlation functions $f^{\rm II}_{1\Omega'}(\tau_{ws};\beta)$ are modular forms of $\Gamma(N_{D\Lambda})$, and $f^{\rm II}_{1\Omega'}(N_{D\Lambda}\tau;\beta)$ of $\Gamma_1(N_{D\Lambda}^2)$; when we choose $f_\rho=2$, $N_{D\Lambda}^2=8^2=64$ now. So, we have seen that both perspectives along the upper-right edge and along the upper-left edge in the diagram (16) yield the same modular form.

[35] the ideals that appear in Example 2.1.2 and at the end of section 2.1.3

3.4. The example $[E_z]_{\mathbb{C}}$ with $z = \sqrt{2}i$: $j = 8000$

The vector space $S_2(\Gamma(8))$ of weight-2 cuspforms for $\Gamma(8)$ is of 5-dimensions (e.g., [20]); the remaining 2-dimensional vector space is generated by 2 modular forms that correspond to the arithmetic model of $[E_{z=\sqrt{2}i}]_{\mathbb{C}}$ that we explained in Example 2.1.3 (the field of definition k is a degree-2 extension over $K = \mathbb{Q}(\sqrt{-2})$). In the language of string theory, on the other hand, we can think of the vector space $F([z], f_\rho)$ of the chiral correlation functions for the target space with $([z], f_\rho) = ([\sqrt{2}i], 1)$; the level of the quadratic form $N_{D\Lambda}$ is 8 in this case, so the vector space $F([\sqrt{2}i], 1)$ is also identified within $S_2(\Gamma(8))$. We have seen that a story holds for the remaining 2-dimensional subspace of $S_2(\Gamma(8))$ in complete parallel to the 3-dimensional subspace $S_2(\Gamma_0(64))$ of $S_2(\Gamma(8)) \cong S_2(\Gamma_1(64))$ in section 3.3. More details of this story is written down in the preprint version [17, Example 2.4.17 and §3.2.1].

4. Newforms from the chiral correlation functions

4.1. The formula for newforms

Let us fix a pair of $\mathcal{O}_{f_z=1} = \mathcal{O}_K$ and f_ρ. On one hand, in Type II string theory, we have $h(\mathcal{O}_K)$ rational SCFT's, and the vector space of their chiral correlation functions

$$\oplus_{a=1,\cdots,h(\mathcal{O}_K)} F([z_a], f_\rho) =: F(\mathcal{E}ll(\mathcal{O}_K), f_\rho). \tag{29}$$

We have seen that this vector space is a part of

$$S_2(\Gamma(N_{D\Lambda})) \subset S_2(\Gamma_1(N_{D\Lambda}^2)).$$

On the other hand, let $\underline{\mathfrak{c}} = (f_\rho\sqrt{D_K})_{\mathcal{O}_K}$ be the ideal of $\mathcal{O}_K$ common to all the $h(\mathcal{O}_K)$ rational SCFT's (see section 3.2). For ideals $\mathfrak{c}_f$ that divides $\underline{\mathfrak{c}}$, one may list up all the elliptic curves of Shimura type of $[E_{z_a}]_{\mathbb{C}}$'s in $\mathcal{E}ll(\mathcal{O}_K)$, as we have explained in section 2.1.3; there are only finite number of such arithmetic models. The weight-2 modular forms that correspond to those arithmetic models, as in section 2.1.4, are found in

$$S_2(\Gamma_1(|D_K|\mathrm{Nm}_{K/\mathbb{Q}}(\underline{\mathfrak{c}}))).$$

They are the same vector space, because (see (15) and (18))

$$N_{D\Lambda}^2 = (f_\rho|D_K|)^2, \tag{30}$$

$$|D_K|\mathrm{Nm}_{K/\mathbb{Q}}(\underline{\mathfrak{c}}) \; = |D_K|\mathrm{Nm}_{K/\mathbb{Q}}((f_\rho\sqrt{D_K})_{\mathcal{O}_K}) = |D_K|f_\rho^2|D_K|.$$

The route through the upper-left edge of the diagram (16) in the language of string theory systematically yields objects in the same vector space as the theory of modular parametrization (the upper-right edge of (16)) does.

For all those elliptic curves of Shimura-type, we have found a formula for their modular forms expressed in terms of the chiral correlation functions. The proof involves frequent use of basic algebraic number theory, so we omit the proof in this journal version here, as we set string theorists as primary audience. Interested readers might refer to the preprint version [17, §3.3 and §3.4] for more information. Here, only **the formula** is written down in the following.

Let $[E_{z_a}]_{\mathbb{C}} \in \mathcal{E}ll(\mathcal{O}_K)$, and E its arithmetic model of Shimura type defined over k, where k is an abelian extension of K containing H_K. Let $\{\chi'_f\}$ be the set of $[k : H_K]$ characters of $[\mathcal{O}_K/\mathfrak{c}_f]^\times$ that correspond to the model E/k (see section 2.1.3). The theory of modular parametrization for such an E/k in section 2.1.4 assigns $[k : K]$ weight-2 modular forms. It is possible to express them by using the chiral correlation functions $f^{\rm II}_{1\Omega'}(\tau_{ws};\beta)$ of the rational SCFT's with the set of target spaces $(\mathcal{E}ll(\mathcal{O}_K), f_\rho)$, when the ideal $\mathfrak{c}_f$ divides $\underline{\mathfrak{c}} = (f_\rho\sqrt{D_K})_{\mathcal{O}_K}$. They are given by

$$\sum_{a=1}^{h(\mathcal{O}_K)} \frac{c'_a\sqrt{a_{z_a}}}{\varphi(\mathfrak{b}'_{z_a})} \sum_{[\beta_*]\in iReps_a/[\mathcal{O}_K/\underline{\mathfrak{c}}]^\times} \#([\mathcal{O}_K/\underline{\mathfrak{c}}]^\times_{\beta_*})\; \chi'_f(c'_a a_{z_a}\Omega(\beta_*)) \\ f^{\rm II}_{1\Omega'}(\tau_{ws};[\beta_*];(\chi'_f)^{-1})_{(z_a,f_\rho)}\frac{f_\rho\sqrt{D_K}}{\sqrt{2f_\rho}}. \tag{31}$$

We should explain notations used in the formula (31). Remember that there is one-to-one correspondence between the set $\mathcal{E}ll(\mathcal{O}_K)$ and Cl_K as explained in 2.1.1; $[E_{z_a}]_{\mathbb{C}} = \mathbb{C}/\mathfrak{b}_{z_a} \in \mathcal{E}ll(\mathcal{O}_K)$ is assigned to the ideal class $[\mathfrak{b}_{z_a}] =: \mathfrak{K}_a^{-1} \in \mathrm{Cl}_K$. The first sum over the ideal classes $\mathfrak{K}_a^{-1} \in \mathrm{Cl}_K$ is also a sum of the chiral correlation functions $f^{\rm II}_{1\Omega'}$ of rational SCFT's of $h(\mathcal{O}_K)$ distinct choices of the target space, $([E_{z_a}]_{\mathbb{C}}, f_\rho)$ with $[E_{z_a}]_{\mathbb{C}} \in \mathcal{E}ll(\mathcal{O}_K)$. For each $a \in \{1,\cdots,h(\mathcal{O}_K)\}$, one chooses an element $c'_a \in K$ arbitrarily so that the ideal $c'_a a_{z_a}\mathfrak{b}_{z_a} =: \mathfrak{b}'_{z_a}$ is integral and prime to the ideal $\mathfrak{c}_f$ (if this is too abstract, see the Example in section 4.2.1). Finally, φ is such[36] that

[36] φ is a *Hecke character of K of type* $[-1/2;1,0]$ with the conductor $\mathfrak{c}_f$, if we allow ourselves to use a bit of jargon. The Example in section 4.2.1 will illustrate what φ is like, but interested readers might also have a look at textbooks in algebraic

assigns a complex number $\varphi(\mathfrak{a})$ to an ideal $\mathfrak{a}$ of $\mathcal{O}_K$ prime to $\mathfrak{c}_f$ so that $\varphi(\mathfrak{a}_1\mathfrak{a}_2) = \varphi(\mathfrak{a}_1)\varphi(\mathfrak{a}_2)$ and $\varphi((\alpha)) = \chi'_f(\alpha)\rho^1(\alpha)$ for an ideal $\mathfrak{a} = (\alpha)_{\mathcal{O}_K}$.

We have started out with $[k : H_K]$ characters χ'_f, and there are $[H_K : K]$ choices of φ for each χ'_f (see section 4.2.1 (or [16, §4.2]) for more explanation), so there are $[k : K]$ linear combinations of the chiral correlation functions of the form (31). They are the $[k : K]$ weight-2 modular forms associated with the arithmetic models of Shimura-type $\{E_{z_a}/k \mid a = 1, \cdots, h(\mathcal{O}_K)\}$ of $\{[E_{z_a}]_{\mathbb{C}}\} = \mathcal{E}ll(\mathcal{O}_K)$ associated with the set of $[k : H_K]$ characters $\{\chi'_f\}$.

The formula above reduces to (26, 25) for the two arithmetic models $E_{32A2} \otimes K$ and $E_{64A1} \otimes K$ in Example 2.1.2. That is because $h(\mathcal{O}_K) = 1$ for $K = \mathbb{Q}(\sqrt{-1})$, we can choose $c'_a = a_z = 1$, $\mathfrak{b}_z = \mathfrak{b}'_z = \mathcal{O}_K$, and $\varphi(\mathfrak{b}'_z) = 1$, first of all. The second sum in the formula (31) is over the CM group orbits (23, 24), but $\chi'_{f;32A/64A}(1+i) = 0$, so only the orbit $\mathrm{orb}_{\mathfrak{q}=\mathcal{O}_K}$ represented by $\Omega(\beta_*) = 1$ contributes, where $\chi'_{f;32A/64A}(1) = 1$. The CM group $[\mathcal{O}_K/\underline{\mathfrak{c}}]^\times$ acts on this orbit faithfully, so the isotropy group is trivial. So, the formula (31) is a generalization of what we have done in (26, 25).

4.2. Observation 3: summing over target spaces in $\mathcal{E}ll(\mathcal{O}_K)$

The formula (31) for the $[k : K]$ weight-2 modular forms for an arithmetic model of Shimura type E/k requires summing the chiral correlation functions $f^{\mathrm{II}}_{1\Omega'}(\tau;\beta)_{(z_a,f_\rho)}$ of rational SCFT's with $h(\mathcal{O}_K)$ distinct target spaces, $\{([E_{z_a}], f_\rho) \mid [E_{z_a}]_{\mathbb{C}} \in \mathcal{E}ll(\mathcal{O}_K)\}$. It is certainly not the most natural thing for physicists to do in a quantum field theory; we do not often sum up scattering amplitudes of QFT's with different Lagrangians. The formula (31) says, however, that we should better sum them up to get the modular forms associated with the L-functions of the Galois representations of the arithmetic models.

Back in the argument in section 2.1.4, however, the $[k : K]$ weight-2 modular forms are introduced in association with the $[k : K]$ representations of $\mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})$; those representations in turn were introduced on the vector space (9) and its pull-back by ν^*. Those modular forms and representations are not just for one arithmetic model E/k of $[E]_{\mathbb{C}} \in \mathcal{E}ll(\mathcal{O}_K)$, but for $[H_K : K]$ arithmetic models $\{{}^\sigma E \mid \sigma \in \mathrm{Gal}(k/K)/\mathrm{Gal}(k/H_K) \cong \mathrm{Gal}(H_K/K)\}$.

number theory, or a review in [16, §4.2] for a shortcut.

Arbitrariness in the choice of $c'_a \in K$ cancels in the expression (31), because changing c'_a to $c'_a\alpha \in K$ by $\alpha \in \mathcal{O}_K$ results in changing the factor $\varphi(\mathfrak{b}'_{z_a})$ in the denominator to $\varphi(\mathfrak{b}'_{z_a})\alpha\chi'_f(\alpha)$.

So, the $[k : K]$ modular forms being associated with arithmetic models of $h(\mathcal{O}_K)$ distinct CM elliptic curves over $\mathbb{C}$, ${}^\sigma E \otimes \mathbb{C}$, it is a natural thing than strange thing that their formula exploits rational SCFT correlation functions of $h(\mathcal{O}_K)$ distinct target spaces.

4.2.1. An example with $K = \mathbb{Q}(\sqrt{-5})$ Let us illustrate the formula (31) here, especially in the aspect of summing over different target spaces, by a few examples. No non-trivial information is added on top of the formula (31), so busy readers lose nothing by skipping this section 4.2.1.

Let us choose the parameter $f_\rho = 1$, and think of two target spaces $([E_z]_\mathbb{C}, f_\rho) = ([E_{z_0}]_\mathbb{C}, 1)$ and $([E_{z_1}]_\mathbb{C}, 1)$, where $[E_{z_a}]_\mathbb{C}$ with $a = 0, 1$ constitute $\mathcal{E}ll(\mathcal{O}_K)$ with $K = \mathbb{Q}(\sqrt{-20})$, as in (4). Then the ideal $\underline{\mathfrak{c}}$ of $\mathcal{O}_K$ for the corresponding set of $h(\mathcal{O}_K) = 2$ rational SCFT's is $(\sqrt{-20})_{\mathcal{O}_K}$. Now, the formula (31) ensures that the vector space (29) contains the $h(\mathcal{O}_K) \times [k : H_K] = 2 \times 2$-plet of weight-2 modular forms for each one of the two of the $h(\mathcal{O}_K)$-plet of k-isomorphism classes of arithmetic models of Shimura type illustrated in Example 2.1.4; this is because the conductor of the two $h(\mathcal{O}_K)$-plet of models, $(2\sqrt{5}i)_{\mathcal{O}_K}$ and $(\sqrt{5}i)_{\mathcal{O}_K}$, both divide $\underline{\mathfrak{c}}$.

The expression (31) is just a linear combination of the chiral correlation functions, but their coefficients cannot be worked out while avoiding algebraic number theory altogether. So, here is a pedagogical explanation of how to use the formula (31) for readers with little familiarity on algebraic number theory. First, note that $z_0 = w_K := \sqrt{5}i$ and $z_1 = (1 + w_K)/2$, which means that $(a_{z_a}, b_{z_a}, c_{z_a})$ is $(1, 0, 5)$ and $(2, -2, 3)$ for $a = 0$ and 1, respectively. Second, the ideal $a_{z_a}\mathfrak{b}_{z_a}$ is $\mathcal{O}_K$ for $a = 0$ and $\langle 2, 1 + w_K\rangle =: \mathfrak{p}_2$ for $a = 1$; more background material is found in this footnote.[37] We may choose $c'_a \in K^\times$ as $c'_0 = 1$ and $c'_1 = (1 + w_K)/2$, so that $\mathfrak{b}'_{z_0} = \mathcal{O}_K$ and $\mathfrak{b}'_{z_1} = \mathfrak{p}_{3+}$ are both prime to the ideal $\underline{\mathfrak{c}} = (2w_K)_{\mathcal{O}_K} = \mathfrak{p}_2^2\mathfrak{p}_5$.

[37] Here is a bit of technical details of the prime ideal decomposition of the ring $\mathcal{O}_K = \mathbb{Z}+\mathbb{Z}w_K$, where $w_K = \sqrt{5}i$. Such ideals as $(p)_{\mathcal{O}_K} =: \mathfrak{p}_p$ with $p = 11, 13, 17, 19$ are prime in the ring $\mathcal{O}_K$, and are principal ideals. On the other hand, the ideals $(2)_{\mathcal{O}_K}$, $(5)_{\mathcal{O}_K}$, and $(p)_{\mathcal{O}_K}$ with $p = 3, 7$ are not prime in the ring $\mathcal{O}_K$. Their prime ideal decomposition is as follows: $(2)_{\mathcal{O}_K} = \mathfrak{p}_2^2$, where $\mathfrak{p}_2 := \langle 2, 1 + w_K\rangle$; $(5)_{\mathcal{O}_K} = \mathfrak{p}_5^2$, where $\mathfrak{p}_5 := (w_K)_{\mathcal{O}_K}$; $(p)_{\mathcal{O}_K} = \mathfrak{p}_{p+}\mathfrak{p}_{p-}$ for $p = 3, 7$, where $\mathfrak{p}_{p\epsilon} := \langle p, r_p + \epsilon w_K\rangle$ with $r_3 = 1$ and $r_7 = 3$. The ideal $\mathfrak{p}_5$ is principal. The ideals $\mathfrak{p}_2$ and $\mathfrak{p}_{p\epsilon}$ with $p = 3, 7$ and $\epsilon = \pm$ are not principal, but any product of even number of them is principal. For example, $\mathfrak{p}_2\mathfrak{p}_{3+} = (1 + w_K)_{\mathcal{O}_K}$, which we used in the main text.
The ideal class group $\mathrm{Cl}_K \cong \mathbb{Z}/2\mathbb{Z}$ consists of two ideal classes; the trivial element $\mathfrak{K}_0$ of $\mathbb{Z}/2\mathbb{Z}$ is the class of principal ideal, represented e.g., by $\mathcal{O}_K = a_{z0}\mathfrak{b}_{z_0}$; the non-trivial element $\mathfrak{K}_1$ of $\mathbb{Z}/2\mathbb{Z}$ is the class of ideals of the form of $\mathfrak{p}_2 \times (\alpha)_{\mathcal{O}_K}$ for $\alpha \in K^\times$, represented by any one of $\mathfrak{p}_2 = a_{z_1}\mathfrak{b}_{z_1}$ and $\mathfrak{p}_{p\epsilon}$ with $p = 3, 7$ and $\epsilon = \pm$.

Now, let us work out the coefficients in (31), not for all the $4h(\mathcal{O}_K)$ modular forms corresponding to the four characters $\{\chi'_f(0,\pm 1)\}$ and $\{\chi'_f(1,\pm 1)\}$, but only for $h(\mathcal{O}_K)$ of them corresponding to $\chi'_f(0,1)$ in the following. All the three omitted ones can be worked out in just as elementary procedures, and the results are found in the preprint version [17, §3.4].

The first thing to work out is the values of $\varphi(\mathfrak{b}'_{z_a})$. For $\mathfrak{b}'_{z_0} = \mathcal{O}_K = (1)_{\mathcal{O}_K}$, which is a principal ideal, $\varphi(\mathfrak{b}'_{z_0}) = \rho^1(1)\chi'_f(0,1)(1) = 1$. For $\mathfrak{b}'_{z_1} = \mathfrak{p}_{3+}$, we use the fact that $\mathfrak{p}_{3+}^2 = (-2+w_K)_{\mathcal{O}_K}$; the square of $\varphi(\mathfrak{p}_{3+})$ should be $\varphi((-2+w_K)_{\mathcal{O}_K}) = \rho^1(-2+w_K)\chi'_f(0,1)(-2+w_K)$, which is equal[38] to $\sqrt{5}+2i$; therefore, the $h(\mathcal{O}_K) = 2$ choices of the value of $\varphi(\mathfrak{b}'_{z_1})$ are $\pm e^{-\pi i/4}(1+w_K)/\sqrt{2}$.

In the case of the character $\chi'_f = \chi'_f(0,1)$, the CM-group diagonal combinations of the chiral correlation functions (21) are non-zero only for just one orbit from each rational SCFT, the CM-group orbit of $\Omega(\beta) = 1$ in the theory with the target space $([E_{z_0}]_{\mathbb{C}}, 1)$, and that of $\Omega(\beta) = (7+w_K)/2$ for the target space $([E_{z_1}]_{\mathbb{C}}, 1)$; more systematic account for which orbits contribute and which do not is found in the preprint version [17, Thm. 3.3.10]. For those orbits, the CM group acts faithfully, so $\#(\mathcal{O}_K/\underline{\mathfrak{c}}]^\times_\beta) = 1$. To compute the coefficient $\chi'_f(c'_a a_{z_a}\Omega(\beta))$ for those two orbits, note that $c'_0 a_0 \Omega(\beta)_{\in iReps_0} = 1$, and $c'_1 a_{z_1}\Omega(\beta)_{\in iReps_1} = (1+w_K)/2 \times 2 \times (7+w_K)/2 = (1+4w_K) \equiv 1 \mod \underline{\mathfrak{c}}$. So, $\chi'_f(c'_a a_{z_a}\Omega(\beta)_{\in iReps_a}) = 1$ for both $a = 0,1$. Therefore, the formula (31) for the $h(\mathcal{O}_K) = 2$ modular forms in question is read as

$$\left(f^{\rm II}_{1\Omega'}([1]; \chi_f(0,-1))_{([z_0],1)} \pm e^{\pi i/4} f^{\rm II}_{1\Omega'}([(7+w_K)/2]; \chi_f(0,-1))_{([z_1],1)} \right) \frac{f_\rho \sqrt{D_K}}{\sqrt{2 f_\rho}}.$$

It is straightforward to write down $f^{\rm II}_{1\Omega'} \sim \vartheta^{1\Omega'}_\Lambda$ as a power series of q, so we do not do that in this journal version. Interested readers might have a look at the preprint version [17, §3.4] for the concrete expressions of the modular forms for those arithmetic models.

All those derivations are nothing more than elementary computations faithful to introductory textbooks on algebraic number theory, so we did not include all those details in the preprint version [17, §3.4]. The preprint version (§3.4) and this journal version (section 4.2.1) are complementary in their presentation, and we wish both versions are useful to readers with different background.

[38]The value of the character $\chi'_f(0,1)$ is determined by noting that $(-2+w_K)$ is equal to $(4+w_K)\cdot 3^3$ in the ring $[\mathcal{O}_K/\underline{\mathfrak{c}}]$, so $\chi'_f(0,1)(-2+w_K) = (-1)^0(i)^3 = -i$.

4.3. Observation 4: direct limits along the Kähler parameters

The discussion so far focused on one modular curve at a time, and also one choice of f_ρ for the target space metric in string theory at a time. In this section 4.3, however, we let them scan; that will make it possible to state the theory of modular parametrization and its string-theory counter part for infinitely many arithmetic models of Shimura type all at once.

Let us begin with the following observation. Think of an arithmetic model $E/\mathbb{Q}$ as in section 1.1, or an arithmetic model E/k of Shimura type as in section 2.1.4. Whenever there is a surjective map $\nu'_N : X_0(N) \to_{/\mathbb{Q}} E/\mathbb{Q}$ or $\nu'_N : X_1(N) \otimes K \to_{/K} B/K$, there is also a surjective map $\nu'_M : X_0(M) \to_{/\mathbb{Q}} E/\mathbb{Q}$ and $\nu'_M : X_1(M) \otimes K \to_{/K} B/K$ for any M divisible by N, so that they are compatible with a map $\pi_{M|N} : X_0(M) \to_{/\mathbb{Q}} X_0(N)$ and $\pi_{M|N} : X_1(M) \to_{/\mathbb{Q}} X_1(N)$, respectively. This situation is described as existence of a map

$$\nu' : \varprojlim_{N \in \mathbb{N}} X_0(N) \to_{/\mathbb{Q}} E/\mathbb{Q}, \qquad \nu' : \varprojlim_{N \in \mathbb{N}} (X_1(N) \otimes K) \to_{/K} B/K$$

defined over $\mathbb{Q}$ and K, respectively. Here, the set of integers $\{N \in \mathbb{N}\}$ forms a directed partially ordered set, with the ordering $N \leq M$ introduced if and only if $N|M$.

The 1-forms on $E/\mathbb{Q}$ and B/K supporting the Galois representations may be pulled back to individual modular curves, but they can also be pulled back all the way to the projective limit of the curves:

$$\nu'^{*} : H^{1,0}(B \otimes_K \mathbb{C}; \mathbb{C}) \to \varinjlim_{N \in \mathbb{N}} H^{1,0}(X_1(N) \otimes \mathbb{C}; \mathbb{C}) \cong \varinjlim_{N \in \mathbb{N}} S_2(\Gamma_1(N)). \tag{32}$$

So far, this is just a story in mathematics that adds little to what we have stated in section 2.1.4.

Now, how does this story look like in the language of string theory? First, for a fixed parameter f_ρ of the metric of the target space, the vector space $F(\mathcal{E}ll(\mathcal{O}_K), f_\rho)$ is regarded as a fixed subspace

$$F(\mathcal{E}ll(\mathcal{O}_K), f_\rho) \hookrightarrow S_2(\Gamma_1(N_{D\Lambda}^2)) \hookrightarrow \varinjlim_{N \in \mathbb{N}} S_2(\Gamma_1(N)).$$

Furthermore, one may realize that both the two vector spaces

$$\varinjlim_{N \in \mathbb{N}} S_2(\Gamma_1(N)) \tag{33}$$

and

$$\lim_{\substack{\longrightarrow \\ f_\rho \in \mathbb{N}}} F(\mathcal{E}ll(\mathcal{O}_K), f_\rho) \tag{34}$$

have a similar structure, where the *level of modular forms* M_f and the parameter f_ρ play a similar role (correspondence between them is more like $M_f \sim |D_K|^2 f_\rho^2$ than $M_f \propto f_\rho$); in the vector space (34), the parameters f_ρ governing the target space metric and B-field are regarded as a directed partially ordered set, with the partial ordering $f_\rho \leq f'_\rho$ introduced if and only if $f_\rho | f'_\rho$. One may think that

$$\lim_{\substack{\longrightarrow \\ f_\rho \in \mathbb{N}}} F(\mathcal{E}ll(\mathcal{O}_K), f_\rho) \subset \lim_{\substack{\longrightarrow \\ N \in \mathbb{N}}} S_2(\Gamma_1(N))$$

is the vector space of the chiral correlation functions $f^{\mathrm{II}}_{1\Omega'}(\beta)$, with the $h(\mathcal{O}_K)$ target spaces $\mathcal{E}ll(\mathcal{O}_K)$ with all kinds of complexified Kähler parameters labeled by $f_\rho \in \mathbb{N}$. By letting the Kähler parameter scan, we obtain a set of observables that does not depend on the choice of metric, but depends only on the complex structure of the target space(s).

The statement behind the formula presented in section 4.1 can be restated as follows. For any arithmetic model E/k of Shimura type of a CM elliptic curve $[E_z]_\mathbb{C}$ over $\mathbb{C}$, the 1-forms $H^{1,0}(B;\mathbb{C})$ pulled backed by the surjective map over K (i.e., modular parametrization) are found within the subspace (34) of (33), which is interpreted as string-theory observables with the target space $\mathcal{E}ll(\mathcal{O}_K)$.

$$\nu'^{*}\left(H^{1,0}(B;\mathbb{C})\right) \subset \lim_{\substack{\longrightarrow \\ f_\rho \in \mathbb{N}}} F(\mathcal{E}ll(\mathcal{O}_K), f_\rho).$$

Appendix

A.1. Minimum on modular forms and modular curves

A.1.1. Congruence subgroups There are a few series of subgroups of $\mathrm{SL}(2;\mathbb{Z})$ that have a dedicated notation.

Definition A.1.1. Let N be a positive integer.

$$\Gamma(N) := \left\{ \begin{bmatrix} a & b \\ c & d \end{bmatrix} \in \mathrm{SL}(2;\mathbb{Z}) \;\middle|\; b, c \equiv 0(N),\ a, d \equiv 1(N) \right\}, \tag{35}$$

$$\Gamma_1(N) := \left\{ \begin{bmatrix} a & b \\ c & d \end{bmatrix} \in \mathrm{SL}(2;\mathbb{Z}) \;\middle|\; c \equiv 0(N),\ a, d \equiv 1(N) \right\}, \tag{36}$$

$$\Gamma_0^0(N) := \left\{ \begin{bmatrix} a & b \\ c & d \end{bmatrix} \in \mathrm{SL}(2;\mathbb{Z}) \;\middle|\; b, c \equiv 0(N),\ a, d \in [\mathbb{Z}/(N)]^\times \right\}, \tag{37}$$

$$\Gamma_0(N) := \left\{ \begin{bmatrix} a & b \\ c & d \end{bmatrix} \in \mathrm{SL}(2;\mathbb{Z}) \;\middle|\; c \equiv 0(N),\ a, d \in [\mathbb{Z}/(N)]^\times \right\}, \tag{38}$$

so $\Gamma(N) \subset \Gamma_1(N) \subset \Gamma_0(N)$ and $\Gamma(N) \subset \Gamma_0^0(N) \subset \Gamma_0(N)$. $\Gamma(N)$ is a normal subgroup of $\mathrm{SL}(2;\mathbb{Z})$, and hence also that of any subgroup of $\mathrm{SL}(2;\mathbb{Z})$ that contains $\Gamma(N)$.

All those subgroups can be regarded as special cases of a more general class of subgroups ([26, §3.3] and [19, §9.1])

$$\Gamma(H, N, M) := \left\{ \begin{bmatrix} a & b \\ c & d \end{bmatrix} \in \mathrm{SL}(2;\mathbb{Z}) \;\middle|\; c \equiv 0(N),\ b \equiv 0(M),\ a, d \in H \right\}$$

where N and M are positive integers, and H is a subgroup of the multiplicative group $[\mathbb{Z}/(NM)]^\times$. $\Gamma(N)$ corresponds to the case of $M = N$ and $H = H_N$, where

$$H_N := \{1, N+1, 2N+1, \cdots, N^2 - N + 1\} \subset [\mathbb{Z}/(N^2)]^\times. \tag{39}$$

The subgroup $\Gamma_1(N)$ is reproduced by setting $M = 1$ and $H = \{1\}$, $\Gamma_0^0(N)$ by setting $M = N$ and $H = H_N$, and $\Gamma_0(N)$ by setting $M = 1$ and $H = [\mathbb{Z}/(N)]^\times$. •

Definition A.1.2. A subgroup Γ of $\mathrm{SL}(2;\mathbb{Z})$ is said to be a *congruent subgroup*, if there exists a positive integer N so that $\Gamma(N) \subset \Gamma$.

Lemma A.1.3. There is an isomorphism from $\Gamma(H, N, M)$ to $\Gamma(H, NM, 1)$ given by

$$\begin{bmatrix} a & b \\ c & d \end{bmatrix} \longmapsto \begin{bmatrix} M^{-1} & \\ & 1 \end{bmatrix} \begin{bmatrix} a & b \\ c & d \end{bmatrix} \begin{bmatrix} M & \\ & 1 \end{bmatrix} = \begin{bmatrix} a & b/M \\ cM & d \end{bmatrix}.$$

In particular, this isomorphism identifies $\Gamma(N)$ with $\Gamma(H_N, N^2, 1)$.

A.1.2. The vector space of modular forms

Notation A.1.4. Let $A = [a, b; c, d]$ be an element of $\mathrm{GL}(2;\mathbb{Z})$ with $ad - bc > 0$, and $k \in \mathbb{Z}$. Then $|[A]_k$ is an operator acting on the space of holomorphic functions on $\mathcal{H}$ as follows. For a holomorphic function $f(\tau)$ on $\tau \in \mathcal{H}$,

$f|[A]_k$ is another holomorphic function on $\mathcal{H}$ given by

$$(f|[A]_k)(\tau) := \frac{[\det(A)]^{k/2}}{(c\tau+d)^k} f(A\cdot\tau).$$

The operator $|[A]_k$ is linear on the vector space of holomorphic functions on $\mathcal{H}$.

Definition A.1.5. Let Γ be a congruence subgroup of $\mathrm{SL}(2;\mathbb{Z})$. When a holomorphic function $f(\tau)$ on $\tau \in \mathcal{H}$ satisfies $f|[\gamma]_k = f$ for $\gamma \in \Gamma$, it is said to be a *modular form of weight-k for* Γ. When such a modular form f vanishes at all the cusp points of Γ, it is called a *cuspform*. They form vector spaces over $\mathbb{C}$, and are denoted by $M_k(\Gamma)$ and $S_k(\Gamma)$, respectively.

Lemma A.1.6. The linear operator $|[\mathrm{diag}(N,1)]_k$ induces an isomorphism

$$S_k(\Gamma(N)) \cong S_k(\Gamma(H_N, N^2, 1)).$$

This isomorphism is a special case of $|[\mathrm{diag}(M,1)]_k : S_k(\Gamma(H,N,M)) \to S_k(\Gamma(H,NM,1))$, or even a special case of $|[\mathrm{diag}(r,1)]_k : S_k(\Gamma(H,N,M)) \to S_k(\Gamma(H,Nr,M/r))$ for any positive divisor r of M.

Lemma A.1.7. Let Γ and Γ' be both congruent subgroups of $\mathrm{SL}(2;\mathbb{Z})$. Suppose that Γ is a normal subgroup of Γ'. The group Γ acts trivially (=as identity) on $S_k(\Gamma)$ via the $|[-]_k$ operator; the fact that Γ is a normal subgroup of Γ' can be used to see that $f|[\gamma]_k \in S_k(\Gamma)$ for $f \in S_k(\Gamma)$ and $\gamma \in \Gamma'$, so the group Γ' also acts on the vector space $S_k(\Gamma)$ via $|[-]_k$, but non-trivially. The vector space $S_k(\Gamma)$ can be decomposed under the action of Γ' into the form of

$$S_k(\Gamma) \cong \oplus_{\rho\in iReps(\Gamma'/\Gamma)} S_k(\Gamma',\rho),$$

where $iReps(\Gamma'/\Gamma)$ is the set of irreducible representations of the finite group Γ'/Γ; cusp forms in $S_k(\Gamma',\rho)$ transform under $\gamma \in \Gamma'$ as

$$S_k(\Gamma',\rho) \ni f|[\gamma]_k \longmapsto \rho(\gamma)\cdot f \in S_k(\Gamma',\rho).$$

When a cuspform f belongs to the subspace $S_k(\Gamma',\rho)$, we call the choice of the representation $\rho \in iReps(\Gamma'/\Gamma)$ the *nebentypus* of f.

Here are two examples of this decomposition. The first example is for $\Gamma = \Gamma_1(N)$ and $\Gamma' = \Gamma_0(N)$.

$$S_k(\Gamma_1(N)) \cong \oplus_{\chi_N\in\mathrm{Char}([\mathbb{Z}/(N)]^\times)} S_k(\Gamma_0(N),\chi_N), \tag{40}$$

so χ_N is a Dirichlet character modulo N.

The other example is for $\Gamma = \Gamma(N) \cong \Gamma(H_N, N^2, 1)$ and $\Gamma_0^0(N^2)$. First,

$$S_k(\Gamma(N)) \cong \oplus_{\chi_N \in \mathrm{Char}([\mathbb{Z}/(N)]^\times)} S_k(\Gamma_0^0(N), \chi_N). \tag{41}$$

Due to the isomorphisms

$$\begin{aligned} \Gamma(N) &\cong \Gamma(H_N, N^2, 1), \\ \Gamma_0^0(N) &\cong \Gamma_0([\mathbb{Z}/(N^2)]^\times, N^2, 1) = \Gamma_0(N^2), \end{aligned}$$

we can also recycle the decomposition (40) and use it after replacing N with N^2 to make a statement equivalent to (41). Because the group H_N fits into the chain of subgroups of the multiplicative group $\{1\} \subset H_N \subset [\mathbb{Z}/(N^2)]^\times$, a cuspform for $\Gamma_1(N^2) = \Gamma(\{1\}, N^2, 1)$ is also a cuspform for $\Gamma(H_N, N^2, 1)$ if the nebentypus $\chi : [\mathbb{Z}/(N^2)]^\times \to S^1$ of the cuspform vanishes on $H_N \subset [\mathbb{Z}/(N^2)]^\times$. This idea is schematically written down as

$$S_k(\Gamma(H_N, N^2, 1)) \cong \oplus_{\chi_N \in iReps([\mathbb{Z}/(N)]^\times)} S_k(\Gamma_0(N^2), \chi_N), \tag{42}$$

which is equivalent to (41). SAGE [20] allows us to work out this decomposition (42) explicitly, so we can just translate the result into the language of (41) appropriately. •

A.1.8. We are not going to provide a review on such notions as (the subspace of) oldforms, (the subspace of) newforms, and Hecke operators in this article. Single page is not enough to review those materials for string theorists, while they are quite standard for experts of number theory. We just refer the readers to such textbooks and lecture notes as [9] and [19]. In the following, we quote from those references a result that we refer to in the text, without explaining the jargon.

We begin by stating structure within the vector space $S_2(\Gamma_1(N))$ for positive integer N.

Theorem A.1.9. (e.g., Thm. 5.8.2 of [9]) For any positive integer N, there is a vector subspace of $S_k(\Gamma_1(N))$ called the *space of newforms*, whose definition is found in standard textbooks and lecture notes on modular forms. This subspace is denoted by $[S_k(\Gamma_1(N))]_N^{\mathrm{new}}$, and the modular forms in this subspace is said to be of *level* N. For any nebentypus χ_N, $[S_k(\Gamma_0(N), \chi_N)]_N^{\mathrm{new}}$ is $S_k(\Gamma_0(N), \chi_N) \cap [S_k(\Gamma_1(N))]_N^{\mathrm{new}}$, so

$$[S_k(\Gamma_1(N))]_N^{\mathrm{new}} \cong \oplus_{\chi_N} [S_k(\Gamma_0(N), \chi_N)]_N^{\mathrm{new}}.$$

The Hecke algebra, an algebra over $\mathbb{Z}$ generated by Hecke operators, acts on the individual components $[S_k(\Gamma_0(N), \chi_N)]_N^{\rm new}$ within $S_k(\Gamma_1(N))$, and all the operators in the algebra are diagonalized simultaneously. There is no two simultaneous eigenvectors of the Hecke algebra in $[S_k(\Gamma_0(N), \chi_N)]_N^{\rm new}$ on which the 1-dimensional representation of the Hecke algebra are identical, except when the two eigenvectors are identical except the normalization, so there is no ambiguity in eigenspace decomposition $[S_k(\Gamma_0(N), \chi_N)]_N^{\rm new}$; this property is called the *multiplicity one theorem*. It is conventional to choose each one of those eigenvectors so that its power series expansion in $q = e^{2\pi i\tau}$ begins with the term q (with the coefficient 1). Such eigenvectors in $[S_k(\Gamma_0(N), \chi_N)]_N^{\rm new}$ are called weight-k, level-N *newforms* for $\Gamma_0(N)$ with the nebentypus χ_N. Let $\mathrm{NewForms}(N, \chi_N)$ be the set of those eigenvectors (newforms). •

Theorem A.1.10. (e.g., Thm. 5.8.3 of [9]) Let N be a positive integer. The vector space $S_k(\Gamma_0(N), \chi_N)$ contains a subspace $[S_k(\Gamma_0(N), \chi_N)]_N^{\rm new}$, as stated in Thm. A.1.9; the whole space $S_k(\Gamma_0(N), \chi_N)$ has a structure that is made up of subspaces associated with the vector spaces $[S_k(\Gamma_0(M_f), \chi_N)]_{M_f}^{\rm new}$ labeled by all possible positive integers M_f that divide N. To be more concrete,

$$S_k(\Gamma_0(N), \chi_N) \cong \oplus_{M_f|N} \, [S_k(\Gamma_0(N), \chi_N)]_{M_f} \, ,$$

and the individual components associated with $M_f|N$ are

$$[S_2(\Gamma_0(N), \chi_N)]_{M_f} \;\cong \oplus_{r|(N/M_f)} |[\mathrm{diag}(r,1)]_k \;\; [S_k(\Gamma_0(M_f), \chi_N)]_{M_f}^{\rm new} \, ,$$

$$= \oplus_{f \in \mathrm{NewForms}(M_f, \chi_N)} \oplus_{r|(N/M_f)} \mathbb{C} f|[\mathrm{diag}(r,1)]_k, \tag{43}$$

$$=: \oplus_{f \in \mathrm{NewForms}(M_f, \chi_N)} \, [f]_{M_f}^N. \tag{44}$$

A newform $f \in \mathrm{NewForms}(M_f, \chi_N)$ mapped into $S_k(\Gamma_0(N), \chi_N)$ via the $|[\mathrm{diag}(1,1)]_k$ operator is called a weight-k, level-M_f *newform* for $\Gamma_0(N)$ of nebentypus χ_N.

The set $\mathrm{NewForms}(M_f, \chi_N)$ and the vector space $[S_k(\Gamma_0(M_f), \chi_N)]_{M_f}^{\rm new}$ is empty, if the Dirichlet character $\chi_N : [\mathbb{Z}/(N)]^\times \to S^1$ cannot be induced from a Dirichlet character of $[\mathbb{Z}/(M_f)]^\times$.

The dimension of the vector space $[f]_{M_f}^N$ is the number of divisors of the integer N/M_f, including 1 and (N/M_f).

$$\dim_{\mathbb{C}} \; \left([S_k(\Gamma_0(N), \chi_N)]_{M_f}\right) \\ = |\mathrm{NewForms}(M_f, \chi_N)| \times |\text{divisors of } (N/M_f)|, \tag{45}$$

$$\begin{aligned}(46)\qquad \dim_{\mathbb{C}}\ &(S_k(\Gamma_0(N),\chi_N))\\ &= \sum_{M_f|N} |\mathrm{NewForms}(M_f,\chi_N)| \times |\text{divisors of } (N/M_f)|.\end{aligned}$$

•

Now, let us write down the statement on the structure of the vector space $S_k(\Gamma(H,N,M))$.

Theorem A.1.11. [19, §9.1] Let N and M be positive integers, and H a subgroup of the multiplicative group $[\mathbb{Z}/(NM)]^\times$. In the decomposition and the isomorphisms

$$\begin{aligned} S_k(\Gamma(H,N,M)) &\cong \oplus_{\chi_{NM}} S_k(\Gamma([\mathbb{Z}/(NM)]^\times,N,M),\chi_{NM}),\\ \cong S_k(\Gamma(H,NM,1)) &\cong \oplus_{\chi_{NM}} S_k(\Gamma([\mathbb{Z}/(NM)]^\times,NM,1),\chi_{NM}),\end{aligned}\tag{47}$$

we already have the notion of the subspace of newforms (introduced in Thm. A.1.9)

$$\begin{aligned}(48)\qquad &[S_k(\Gamma([\mathbb{Z}/(NM)]^\times,NM,1),\chi_{NM})]^{\mathrm{new}}_{NM}\\ &\qquad = [S_k(\Gamma_0(NM),\chi_{NM})]^{\mathrm{new}}_{NM} \subset S_k(\Gamma_0(NM),\chi_{NM}),\end{aligned}$$

so we can also introduce the notion of *the subspace of newforms*

$$[S_k(\Gamma(H,N,M))]^{\mathrm{new}}_{NM} \quad \text{and} \quad [S_k(\Gamma([\mathbb{Z}/(NM)]^\times,N,M),\chi_{NM})]^{\mathrm{new}}_{NM}$$

through the identification (47). So long as the character χ_{NM} vanishes on the subgroup $H \subset [\mathbb{Z}/(NM)]^\times$, there is one to one correspondence

$$\begin{aligned} |[\mathrm{diag}(M,1)]_k : \mathrm{NewForms}&(\Gamma([\mathbb{Z}/(NM)]^\times,N,M),\chi_{NM})\\ &\cong \mathrm{NewForms}(\Gamma_0(NM),\chi_{NM}).\end{aligned}$$

The vector spaces $S_k(\Gamma([\mathbb{Z}/(NM)]^\times,N,M),\chi_{NM})$ with the characters χ_{NM} that vanish on a group H have a substructure precisely the same as that of $S_k(\Gamma_0(NM),\chi_{NM})$ stated in Thm. A.1.10; we can just translate the substructure by using the isomorphism $|[\mathrm{diag}(M,1)]_k$.

Of particular interest in this article is the case $M = N$ and $H = H_N$. So, let us write down the result of the translation in the notation for this particular $M = N$ and $H = H_N$ case.

$$S_k(\Gamma^0_0(N),\chi_N) \cong \oplus_{M_f|N^2} \left[S_k(\Gamma^0_0(N),\chi_N)\right]_{M_f}, \tag{49}$$

and the individual components associated with $M_f|N^2$ are

$$
\begin{aligned}
&[S_k\,(\Gamma_0^0(N),\chi_N)]_{M_f}\\
&\qquad\cong \oplus_{r|(N^2/M_f)}|[\mathrm{diag}(N^{-1},1)]_k\cdot|[\mathrm{diag}(r,1)]_k\,[S_k(\Gamma_0(M_f),\chi_N)]^{\mathrm{new}}_{M_f},\\
&\qquad= \oplus_{f\in\mathrm{NewForms}(M_f,\chi_N)}\oplus_{r|(N^2/M_f)}\mathbb{C}f|[\mathrm{diag}(r/N,1)]_k,\\
&\qquad=: \oplus_{f\in\mathrm{NewForms}(M_f,\chi_N)}\,[f]^{N^2,N}_{M_f}.
\end{aligned}
\tag{50}
$$

•

Acknowledgments

The authors are grateful to Scott Carnahan and Yuji Tachikawa for useful comments and discussions. This work is support in part by the World Premier International Research Center Initiative (WPI) and Grant-in-Aid New Area no. 6003, MEXT, Japan.

References

[1] C. Breuil, B. Conrad, F. Diamond, and R. Taylor, "On the modularity of elliptic curves over Q: wilde 3-adic exercises," J. Amer. Math. Soc. **14** (2001) 843–939. MR1839918

[2] P. Candelas, X. de la Ossa and F. Rodriguez-Villegas, "Calabi-Yau manifolds over finite fields. 1.," [arXiv:hep-th/0012233 [hep-th]].
P. Candelas, X. de la Ossa and F. Rodriguez Villegas, "Calabi-Yau manifolds over finite fields. 2.," Fields Inst. Commun. **38** (2013), 121–157 [arXiv:hep-th/0402133 [hep-th]].
P. Candelas, X. de la Ossa, M. Elmi and D. Van Straten, "A One Parameter Family of Calabi-Yau Manifolds with Attractor Points of Rank Two," JHEP **10** (2020), 202 [arXiv:1912.06146 [hep-th]].
P. Candelas, X. De La Ossa and D. Van Straten, "Local Zeta Functions From Calabi-Yau Differential Equations," [arXiv:2104.07816 [hep-th]].
P. Candelas, X. de la Ossa, P. Kuusela and J. McGovern, "Mirror Symmetry for Five-Parameter Hulek-Verrill Manifolds," [arXiv:2111.02440 [hep-th]]. MR2019149

[3] A. Coste and T. Gannon, "Remarks on Galois symmetry in rational conformal field theories," Phys. Lett. B **323** (1994) 316. MR1266785

[4] O. Davidovich, T.J. Hagge, Z. Wang, "On Arithmetic Modular Categories," arXiv:1305.2229 [math.QA].

[5] J. de Boer and J. Goeree, "Markov traces and II_1 factors in conformal field theory," Comm. Math. Phys. **139** (1991) pp.267–304. MR1120140

[6] P. Degiovanni, "Equations de Moore et Seiberg, Theories Topologiques et Theorie de Galois," Helv. Phys. Acta **67** (1994) 799. MR1325107

[7] P. Degiovanni, "Moore and Seiberg equations, topological field theories and Galois theory," an article in [24]. MR1305404

[8] M. Deuring, "Die Zetafunktion einer algebraischen Kurve vom Geschlecht Eins, I, II, III, IV," Nachr. Akad. Wiss. Göttingen, (1953) 85–94, (1955) 13–42, (1956) 37–76, and (1957) 55–80. MR0070666

[9] F. Diamond and J. Shurman, "A First Course in Modular Forms," GTM 228, Springer, 2005. MR2112196

[10] J. Fuchs, B. Gato-Rivera, B. Schellekens and C. Schweigert, "Modular invariants and fusion rule automorphisms from Galois theory," Phys. Lett. B **334** (1994) 113 [hep-th/9405153]. MR1290075

[11] T. Gannon, "Moonshine beyond the Monster" Cambridge monographs on mathematical physics. 2006. MR2257727

[12] C. Goldstein and N. Schappacher, "Series d'Eisenstein et fonctions L de courbes elliptiques a multiplication complexe." (French) [Eisenstein series and L functions of elliptic curves with complex multiplication] J. Reine Angew. Math. 327 (1981), 184–218. MR0631315

[13] S. Gukov and C. Vafa, "Rational conformal field theories and complex multiplication," Commun. Math. Phys. **246** (2004) 181 [hep-th/0203213]. MR2044895

[14] J. A. Harvey and Y. Wu, "Hecke Relations in Rational Conformal Field Theory," JHEP **1809** (2018) 032 [arXiv:1804.06860 [hep-th]]. J. A. Harvey, Y. Hu and Y. Wu, "Galois Symmetry Induced by Hecke Relations in Rational Conformal Field Theory and Associated Modular Tensor Categories," J. Phys. A **53** (2020) no.33, 334003 [arXiv:1912.11955 [hep-th]]. MR4137519

[15] S. Kachru, R. Nally and W. Yang, "Supersymmetric Flux Compactifications and Calabi-Yau Modularity," [arXiv:2001.06022 [hep-th]]. S. Kachru, R. Nally and W. Yang, "Flux Modularity, F-Theory, and Rational Models," [arXiv:2010.07285 [hep-th]].

[16] S. Kondo and T. Watari, "String-theory Realization of Modular Forms for Elliptic Curves with Complex Multiplication," Commun. Math. Phys. **367** (2019) 89 [arXiv:1801.07464 [hep-th]]. MR3933405

[17] S. Kondo and T. Watari, arXiv:1912.13294, which is the preprint (original) version of this study, available from arXiv.

[18] G. Moore, "Arithmetic and attractors," hep-th/9807087.

[19] K. A. Ribet and W. Stein "Lectures on Modular Forms and Hecke Operators", online book, available at https://wstein.org/

[20] SageMath, a free open-source mathematics software system available online.

[21] N. Schappacher, "Periods of Hecke characters." Lecture Notes in Mathematics, 1301. Springer-Verlag, Berlin, 1988. xvi+160 pp. ISBN: 3-540-18915-7 MR0935127

[22] R. Schimmrigk and S. Underwood, "The Shimura–Taniyama Conjecture and Conformal Field Theory," J. Geom. Phys. **48** (2003) 169 [hep-th/0211284].
M. Lynker and R. Schimmrigk, "Geometric Kac–Moody Modularity," J. Geom. Phys. **56** (2006) 843–863 [hep-th/0410189].
R. Schimmrigk, "The Langlands Program and String Modular K3 Surfaces," Nucl. Phys. **B771** (2007) 143–166 [hep-th/0603234].
"Emergent Spacetime from Modular Motives," Comm. Math. Phys. **303** (2011) 1–30 [arXiv:0812.4450 [hep-th]]. MR2217492

[23] R. Schimmrigk, "Arithmetic spacetime geometry from string theory," Int. J. Mod. Phys. A **21** (2006) 6323 [hep-th/0510091]. MR2290256

[24] L. Schneps, "The Grothendieck Theory of Dessins d'Enfants," London Mathematical Society LNS vol. 200, Cambridge U Press, 1994. MR1305390

[25] S. Sehgal "Units in integral group rings," Monographs and Surveys in Pure and Applied Mathematics, Chapman and Hall, 1993. MR1242557

[26] G. Shimura, "Introduction to the Arithmetic Theory of Automorphic Functions," 1971, Iwanami/Princeton U. Press. MR0314766

[27] F. Strömberg, "Weil representation associated with finite quadratic modules," Math. Zeitschrift (2013) **275** 509. MR3101818

[28] S. Wortmann, "Generalized Q-curves and factors of $J_1(N)$." Abh. Math. Sem. Univ. Hamburg 70 (2000), 51–61. MR1809533

Satoshi Kondo
Middle East Technical University, Northern Cyprus Campus
99738 Kalkanli, Guzelyurt, Mersin 10
Turkey
Kavli Institute for the Physics and Mathematics of the Universe
University of Tokyo
Kashiwa-no-ha 5-1-5, 277-8583
Japan
E-mail address: satoshi.kondo@gmail.com

Taizan Watari
Kavli Institute for the Physics and Mathematics of the Universe
University of Tokyo
Kashiwa-no-ha 5-1-5, 277-8583
Japan
E-mail address: taizan.watari @ ipmu.jp

Received September 17, 2020
Accepted March 1, 2022