Available online at www.sciencedirect.com
SCIENCE DIRECT®
ELSEVIER
Journal of Geometry and Physics 48 (2003) 169–189
JOURNAL OF GEOMETRY AND PHYSICS
www.elsevier.com/locate/jgp

The Shimura–Taniyama conjecture and conformal field theory

Rolf Schimmrigk [a,*], Sean Underwood [b]

[a] *Kennesaw State University, 1000 Chastain Road, Kennesaw, GA 30144, USA*
[b] *Georgia Southwestern State University, 800 Wheatley St., Americus, GA 31709, USA*

Received 12 December 2002; accepted 11 February 2003

Abstract

The Shimura–Taniyama conjecture states that the Mellin transform of the Hasse–Weil L-function of any elliptic curve defined over the rational numbers is a modular form. Recent work of Wiles, Taylor–Wiles and Breuil–Conrad–Diamond–Taylor has provided a proof of this longstanding conjecture. Elliptic curves provide the simplest framework for a class of Calabi–Yau manifolds which have been conjectured to be exactly solvable. It is shown that the Hasse–Weil modular form determined by the arithmetic structure of the Fermat type elliptic curve is related in a natural way to a modular form arising from the character of a conformal field theory derived from an affine Kac–Moody algebra.

MSC: 11G25; 11G40; 14G10; 14G40

PACS: 11.25.-w; 11.25.Hf; 11.25.Mj

Subj. Class.: Quantum field theory

Keywords: Varieties over finite fields; L-functions; Zeta functions; Fundamental string theory

1. Introduction

Recent evidence suggests that the string theoretic nature of spacetime can be illuminated by exploring the arithmetic structure of the defining varieties. A first indication of the usefulness of this technique is the identification of the quantum dimensions of the chiral primary fields of exactly solvable string models as certain units of a number field determined by

* Corresponding author. Tel.: +1-7704236591; fax: +1-7704236625.
E-mail addresses: netahu@yahoo.com (R. Schimmrigk), seancu@sowega.net (S. Underwood).

0393-0440/$ – see front matter © 2003 Elsevier Science B.V. All rights reserved.
doi:10.1016/S0393-0440(03)00030-5

the Hasse–Weil L-function of the corresponding Calabi–Yau manifold. This result provides a geometric characterization of the 'fine structure' of the spectrum that goes beyond the usual identification of marginal operators of the conformal field theory with elements of cohomology groups of the variety [1].

Counting states is an issue that can be addressed in any of the different formulations that have been applied to the problem of understanding the relation between Calabi–Yau varieties and conformal field theories, such as Landau–Ginzburg theory [2–4], and the σ-theoretic approach [5]. A question that so far has resisted efforts is how the modularity of the two-dimensional conformal field theory is encoded in the geometry of space-time. More precisely, one wants to understand how the characters of the underlying conformal field theory are determined by the variety itself, and vice versa. It is the purpose of this article to establish this relation in the simplest case of toroidal Calabi–Yau compactifications.

Moral support for this investigation comes from the recent proof of the more than three centuries old conjecture of Fermat's last theorem. The basic ingredient of this proof is a conjecture first put forward by Taniyama [6], sharpened by Shimura [7], and made more concrete by Weil [8] ([9] contains some remarks concerning the interesting history of this conjecture). There are several different ways to formulate this conjecture, but they all lead to a statement to the effect that the arithmetically defined Hasse–Weil L-function of an elliptic curve over the rational numbers is the Mellin transform of a modular form of weight 2 with respect to some congruence subgroup of $\mathrm{SL}(2,\mathbb{Z})$. The geometric background for this result is provided by Shimura's construction, which shows that the Jacobian of an elliptic curve can be recovered as a factor of an abelian variety determined by a modular form of weight 2 and level N [10].

The Shimura–Taniyama conjecture has provided a focal point of much work in arithmetic algebraic geometry over the last few decades. It moved to center stage with Frey's observation [11] that rational solutions of Fermat type plane curves can be used to construct certain special types of semi-stable elliptic curves. Frey argued that the resulting elliptic curves would in fact be so special that they would contradict the Shimura–Taniyama conjecture. Establishing the Shimura–Taniyama conjecture would therefore finally prove Fermat's last theorem. Ribet's proof [12] of Frey's conjecture provided the key motivation for Wiles' attempt to prove the conjecture, and hence Fermat's theorem [13,14]. More recently, the work of Wiles and Taylor–Wiles has been extended to the full Shimura–Taniyama conjecture, avoiding the requirement of semi-stability. Without any constraints on the type of the elliptic curve the following result has been proven in a sequence of papers with an increasing number of authors [15–17]. Denote by $\mathbb{Q}$ the field of rational numbers, by $\mathbb{F}_p$ the finite field of order p, and by $E/\mathbb{F}_p$ the reduced curve E over the field $\mathbb{F}_p$. An elliptic curve E is defined over $\mathbb{Q}$ if all its coefficients are rational numbers. Set $q = \mathrm{e}^{2\pi\mathrm{i}\tau}$.

Theorem (Breuil et al. [17]). *Every elliptic curve E over $\mathbb{Q}$ is modular in the sense that there exists a modular form $f = \sum_{n=1}^{\infty} a_n(f)q^n$ of weight 2 and some level N, determined by the conductor of the elliptic curve, such that the numbers*

$$a_p(E) = p + 1 - \#(E/\mathbb{F}_p) \tag{1}$$

defined by the cardinalities $\#(E/\mathbb{F}_p)$ *of the curve at rational primes* $p \nmid N$ *are related to the coefficients* $a_p(f)$ *of the modular form f as*

$$a_p(E) = a_p(f). \tag{2}$$

Elliptic curves provide the simplest examples in a class of Calabi–Yau manifolds which has been conjectured by Gepner [18] to be exactly solvable in terms of certain two-dimensional $N = 2$ superconformal field theories. Conformal field theories are determined by partition functions whose ingredients are holomorphic characters and multiplicity invariants which link the holomorphic and anti-holomorphic sectors. In the context of elliptic Calabi–Yau manifolds the most elementary exactly solvable example is the cubic plane curve embedded in the projective plane

$$C_3 = \{(z_0 : z_1 : z_2) \in \mathbb{P}_2 | z_0^3 + z_1^3 + z_2^3 = 0\}. \tag{3}$$

The underlying conformal field theory of this curve is thought to be derived from the affine SU(2) Lie algebra at level $k = 1$

$$\mathbb{P}_2 \supset C_3 \cong (\mathrm{SU}(2)_{k=1,A_1})^{\otimes 3}_{\mathrm{GSO}}, \tag{4}$$

where A_1 signifies the diagonal invariant for the SU(2) partition function, and GSO indicates the projection which guarantees integral U(1)-charges of the states. The main ingredient of the partition function of this theory is the string function $c(\tau)$ which determines the character $\kappa(\tau)$ of the parafermionic theory at level $k = 1$ via $\kappa(\tau) = \eta(\tau)c(\tau)$, where $\eta(\tau) = q^{1/24}\prod_{n=1}^{\infty}(1 - q^n)$ is the Dedekind function. The parafermionic theory in turn determines the $N = 2$ superconformal minimal models. Alternatively, one can obtain the supersymmetric theory via the Goddard–Kent–Olive coset construction.

The goal of this paper is to show that the theta functions determined by the characters of the conformal field theory determine the Hasse–Weil L-function in a simple way. More precisely, it is shown that the following holds. Denote by $S_2(\Gamma_0(N))$ the set of cusp forms of the congruence group of elements of $\mathrm{SL}(2, \mathbb{Z})$ that are upper triangular mod N

$$\Gamma_0(N) = \left\{ \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \mathrm{SL}_2(\mathbb{Z}) \middle| \begin{pmatrix} a & b \\ c & d \end{pmatrix} \sim \begin{pmatrix} * & * \\ 0 & * \end{pmatrix} (\mathrm{mod}\ N) \right\}. \tag{5}$$

Theorem. *The Mellin transform of the Hasse–Weil L-function* $L_{\mathrm{HW}}(C_3, s)$ *of the cubic elliptic curve* $C_3 \subset \mathbb{P}_2$ *is a modular form* $f_{\mathrm{HW}}(C_3, q) \in S_2(\Gamma_0(27))$ *which factors into the product*

$$f_{\mathrm{HW}}(C_3, q) = \Theta(q^3)\Theta(q^9). \tag{6}$$

Here $\Theta(\tau) = \eta^3(\tau)c(\tau)$ *is the Hecke modular form associated to the quadratic extension* $\mathbb{Q}(\sqrt{3})$ *of the rational field* $\mathbb{Q}$, *determined by the unique string function* $c(\tau)$ *of the affine Kac–Moody* SU(2)*-algebra at conformal level* $k = 1$.

This result provides a string theoretic origin of the Hasse–Weil modular form of the plane cubic Fermat torus in terms of an exactly solvable conformal field theory character determined by an affine SU(2) Kac–Moody algebra.

Even though at present few exactly solvable points are known explicitly, the Shimura–Taniyama conjecture shows that modularity among Calabi–Yau curves is a common phenomenon, not restricted to a few discrete points in moduli space. The link established in this paper between geometrically defined modular forms and conformal field theoretic modular forms, in combination with the proofs of the Shimura–Taniyama conjecture, leads to the conjecture that the space of exactly solvable Calabi–Yau varieties at central charge $c = 3$ is dense in the space of Calabi–Yau curves (see [19] for a different approach to this question). What is needed is a better understanding of the conformal field theory side of this relation.

The outline of this note is as follows. In Section 2 we describe Artin's zeta function and the resulting Hasse–Weil L-function. Section 3 contains a brief summary of some of the pertinent aspects of $N = 2$ superconformal field theories. Section 4 explains the arguments that recover the conformal field theory modular form from the variety, while Section 5 contains some remarks concerning the inverse problem of reconstructing Calabi–Yau varieties from conformal field theory. Section 6 describes an alternative point of view in terms of the representation theory of the absolute Galois group on the torsion points of the elliptic curve.

2. The Hasse–Weil L-function

For reasons explained in [1] it makes sense from a physical perspective to combine the arithmetic information contained at arbitrary prime numbers into a single object, the Hasse–Weil L-function. Such a global object was first introduced by Hasse in the late thirties (he suggested its investigation as a dissertation topic to his student Humbert [20]), and later reformulated by Weil [21,22]. The starting point for the Hasse–Weil L-function of an algebraic curve X is the local congruent zeta function at a prime number p, defined by Weil [23] as the generating series

$$Z(X/\mathbb{F}_p, t) \equiv \exp\left(\sum_{r\in\mathbb{N}} \#(X/\mathbb{F}_{p^r})\frac{t^r}{r}\right) \tag{7}$$

in terms of a formal variable t. In a somewhat different formulation this function was introduced by Artin [24] and Schmidt [25]. This arrangement of the cardinalities $\#(X/\mathbb{F}_{p^r})$ is motivated by the idea to translate additive properties of these numbers into a multiplicative structure of the generating function. It was first shown by Schmidt [26–28] that $Z(X/\mathbb{F}_p, t)$ is a rational function which takes the form

$$Z(X/\mathbb{F}_p, t) = \frac{\mathcal{P}^{(p)}(t)}{(1-t)(1-pt)}, \tag{8}$$

where $\mathcal{P}^{(p)}(t)$ is a function whose degree is independent of the prime p and is given by the genus $g(X)$ of the curve, $\deg(X) = 2g(X)$. It was later recognized that the structure indicated by this simple expression holds quite generally in the sense that the zeta function splits into factors determined by the de Rham cohomology groups $H_{\mathrm{dR}}(X)$ of a variety X (see [29] for a beautiful historical introduction to this subject).

More important from a physical perspective is the global zeta function, obtained by setting $t = p^{-s}$ and taking the product over all rational primes at which the variety has good reduction. Denote by S the set of rational primes at which X becomes singular and denote by P_S the set of primes that are not in S. The global zeta function can be defined as

$$Z(X,s) = \prod_{p\in P_S} \frac{\mathcal{P}^{(p)}(p^{-s})}{(1-p^{-s})(1-p^{1-s})} = \frac{\zeta(s)\zeta(s-1)}{\prod_{p\in P_S} L_p(X,s)} \tag{9}$$

where the local L-function has been defined as

$$L_p(X,s) = \frac{1}{\mathcal{P}^{(p)}(p^{-s})} \tag{10}$$

and $\zeta(s) = \prod_p (1-p^{-s})^{-1}$ is the Riemann zeta of the rational field $\mathbb{Q}$. It becomes clear from this way of writing the zeta function that one of the advantages of defining the L-function via Eq. (9) derives from the fact that this expression separates the arithmetic of the variety from that of the rational number field $\mathbb{Q}$.

The factors $\mathcal{P}^{(p)}(t)$ can be analyzed in a number of different ways. The most direct way is to expand Artin's form of the zeta function and compare the coefficients with the expansion of Schmidt's rational form of it. Writing the polynomials $\mathcal{P}^{(p)}(t)$ at the good primes as

$$\mathcal{P}^{(p)}(t) = \sum_{i=0}^{2g} \beta_i(p) t^i, \tag{11}$$

the first few coefficients $\beta_i(p)$ expressed in terms of the $N_{r,p} = \#(X/\mathbb{F}_{p^r})$ are given by

$$\begin{aligned}
&\beta_0(p) = 1,\\
&\beta_1(p) = N_{1,p} - (p+1),\\
&\beta_2(p) = \tfrac{1}{2}(N_{1,p}^2 + N_{2,p}) - (p+1)N_{1,p} + p,\\
&\vdots\\
&\beta_{2g}(p) = p^g.
\end{aligned} \tag{12}$$

At genus $g = 1$ the zeta function is completely determined by $\beta_1(p)$.

Depending on the issues at hand, it might be necessary to complete this definition with factors coming from the bad and infinite primes. The general structure of these factors is described in [30]. For elliptic curves the discussion simplifies considerably. For any prime p the polynomials $\mathcal{P}^{(p)}(t)$ for elliptic curves can be written as

$$\mathcal{P}^{(p)}(t) = 1 + \beta_1(p)t + \delta(p)pt^2 \tag{13}$$

with

$$\delta(p) = \left\{ \begin{array}{ll} 0 & \text{if } p \text{ is a bad prime} \\ 1 & \text{if } p \text{ is a good prime} \end{array} \right\}. \tag{14}$$

At the bad primes the precise structure of the coefficients $\beta_1(p)$ depends on the type of the singularity

Table 1
The coefficients $\beta_1(p) = N_{1,p}(C_3) - (p+1)$ of the elliptic cubic curve C_3 in terms of the cardinalities $N_{1,p}$ for the lower rational primes

	Prime, p										
	2	3	5	7	11	13	17	19	23	29	31
$N_{1,p}$	3	4	6	9	12	9	18	27	24	30	36
$\beta_1(p)$	0	0	0	1	0	−5	0	7	0	0	4

$$\beta_1(p) = \left\{ \begin{array}{ll} \pm 1 & \text{if the singularity at } p \text{ is a node} \\ 0 & \text{if the singularity at } p \text{ is a cusp} \end{array} \right\}. \tag{15}$$

Here the sign in the first case depends on whether the node is split or non-split. The Hasse–Weil L-function can then be defined as

$$L_{\mathrm{HW}}(X,s) = \prod_{p\in S} \frac{1}{1+\beta_1(p)p^{-s}} \prod_{p\in P_S} \frac{1}{1+\beta_1(p)p^{-s}+p^{2-2s}}. \tag{16}$$

Computing the cardinalities $N_{1,p}$ for the cubic curve C_3 given in Eq. (3) explicitly allows to determine the lower terms of the q-series. For the lower primes the computation leads to the results in Table 1.

This leads to a Hasse–Weil series of the cubic elliptic curve

$$L_{\mathrm{HW}}(C_3,s) = 1 - \frac{2}{4^s} - \frac{1}{7^s} + \frac{5}{13^s} + \frac{4}{16^s} - \frac{7}{19^s} + \cdots. \tag{17}$$

A standard maneuver then obtains from the Hasse–Weil L-series of any elliptic curve X

$$L_{\mathrm{HW}}(X,s) = \prod_{p\in S} \frac{1}{1+\beta_1(p)} \prod_{p\in P_S} \frac{1}{1+\beta_1(p)p^{-s}+p^{1-2s}} = \sum_{n=1}^{\infty} a_n n^{-s} \tag{18}$$

an associated q-expansion via the Mellin transform. This map produces for a given q-series $f = \sum_n a_n q^n$ a series $L(s) = \sum_n a_n n^{-s}$ via the integral

$$L(s) = \frac{(2\pi)^s}{\Gamma(s)} \int_0^{\infty} f(\mathrm{i}y) y^{s-1}\, \mathrm{d}y. \tag{19}$$

It effectively replaces $n^{-s} \leftrightarrow q^n$, where $q = \mathrm{e}^{2\pi \mathrm{i}\tau}$, and $\tau \in \mathfrak{H}$ parametrizes the upper half plane. This leads to the Hasse–Weil form

$$f_{\mathrm{HW}}(X,q) = \sum_{n=1}^{\infty} a_n q^n \tag{20}$$

associated to the Hasse–Weil L-series. Applied to the Fermat cubic curve this leads to

$$f_{\mathrm{HW}}(C_3,q) = q - 2q^4 - q^7 + 5q^{13} + 4q^{16} - 7q^{19} + \cdots. \tag{21}$$

Expansions like this often turn out to be useful because of theorems which show that such functions are determined uniquely by a finite number of terms.

This result raises a number of questions. First, we need to know whether $f_{\mathrm{HW}}(C_3, q)$ is a modular form. That it is becomes clear from the proof of the Shimura–Taniyama conjecture because the Fermat cubic can be mapped into a Weierstrass form defined over $\mathbb{Q}$. It then follows from the result (21) that it is a cusp form (since $a_0 = 0$) and that it is normalized (since $a_1 = 1$). We also need to know what its level and weight are. Finally, we need to know whether it is a Hecke eigenform.

The weight of a Hecke eigenform can be read off directly from the multiplicative properties of such a form. This can be seen as follows. Consider the set M_n of 2×2 matrices over $\mathbb{Z}$ with determinant n. For

$$M = \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in M_n$$

and a function f on $\mathfrak{H}$ define

$$(Mf)_k(\tau) = \frac{\det(M)^{k-1}}{(c\tau + d)^k} f(\tau). \tag{22}$$

Define the Hecke operators as

$$T_k(n) = \sum_{M \in M_n / \Gamma(1)} (Mf)_k(\tau). \tag{23}$$

Then

$$\begin{aligned} &T_k(mn) = T_k(m)T_k(n), \quad m, n \text{ coprime}, \\ &T_k(p^{n+1}) = T_k(p^n)T_k(p) - p^{k-1}T_k(p^{n-1}), \quad p \text{ prime}. \end{aligned} \tag{24}$$

A special operator has to be considered at primes p which divide the level N of the form. This is the so-called Atkin–Lehner operator [31], for which no universal notation seems to exist, but which is often denoted by $U_k(p)$

$$U_k(p^n) = (U_k(p))^n. \tag{25}$$

For eigenforms of these operators the operator structure translates into identical relations between their coefficients a_n

$$\begin{aligned} &a_{mn} = a_m a_n \ (m, n) = 1, \qquad a_{p^{n+1}} = a_{p^n} a_p - p^{k-1} a_{p^{n-1}}, \\ &a_{p^n} = (a_p)^n, \quad \text{for } p|N. \end{aligned} \tag{26}$$

The Hasse–Weil form $f_{\mathrm{HW}}(C_3, q)$ of the elliptic cubic curve satisfies these relations with $k = 2$, hence defines a normalized cusp Hecke eigenform of weight 2.

3. Gepner models

The simplest class of $N = 2$ supersymmetric exactly solvable theories is built in terms of the affine SU(2) theory as a coset model

$$\frac{\mathrm{SU}(2)_k \otimes \mathrm{U}(1)_2}{\mathrm{U}(1)_{k+2,\mathrm{diag}}}. \tag{27}$$

Coset theories G/H lead to central charges of the form $c_{\mathrm{G}} - c_{\mathrm{H}}$, hence the supersymmetric affine theory at level k still has central charge $c_k = 3k/(k+2)$. The spectrum of anomalous dimensions $\Delta^{\ell}_{q,s}$ and U(1)-charges Q^{ℓ} of the primary fields $\Phi^{\ell}_{q,s}$ at level k is given by

$$\Delta^{\ell}_{q,s} = \frac{\ell(\ell+2) - q^2}{4(k+2)} + \frac{s^2}{8}, \qquad Q^{\ell}_{q,s} = \frac{q}{k+2} - \frac{s}{2}, \tag{28}$$

where $\ell \in \{0, 1, \ldots, k\}$, $\ell + q + s \in 2\mathbb{Z}$, and $|q - s| \leq \ell$. Associated to the primary fields are characters defined as

$$\begin{aligned}\chi^{\ell}_{q,s,u}(\tau, z) &= \mathrm{e}^{2\pi \mathrm{i} u}\, \mathrm{tr}_{\mathcal{H}^{\ell}_{q,s}} q^{(L_0 - (c/24))}\, \mathrm{e}^{2\pi \mathrm{i} J_0} \\ &= \mathrm{e}^{2\pi \mathrm{i} u} \sum_{Q^{\ell}_{q,s}, \Delta^{\ell}_{q,s}} \mathrm{mult}(\Delta^{\ell}_{q,s}, Q^{\ell}_{q,s})\, \mathrm{e}^{2\pi \mathrm{i}(\Delta^{\ell}_{q,s} - (c/24)) + 2\pi i Q^{\ell}_{q,s}},\end{aligned} \tag{29}$$

where the trace is to be taken over a projection $\mathcal{H}^{\ell}_{q,s}$ to a definite fermion number (mod 2) of a highest weight representation of the (right-moving) $N = 2$ algebra with highest weight vector determined by the primary field. It is of advantage to express these maps in terms of the string functions and theta functions, leading to the form

$$\chi^{\ell}_{q,s}(\tau, z, u) = \sum c^{\ell}_{q+4j-s}(\tau) \Theta_{2q+(4j-s)(k+2), 2k(k+2)}(\tau, z, u) \tag{30}$$

because it follows from this representation that the modular behavior of the $N = 2$ characters decomposes into a product of the affine SU(2) structure in the ℓ index, and into Θ-function behavior in the charge and sector index. The string functions c^{ℓ}_{m} are given by

$$c^{\ell}_{m}(\tau) = \frac{1}{\eta^3(\tau)} \sum_{\substack{-|x| < y \leq |x| \\ (x,y) \text{ or } ((1/2)-x, (1/2)+y) \\ \in \mathbb{Z}^2 + ((\ell+1)/2(k+2), m/2k)}} \mathrm{sign}(x)\, \mathrm{e}^{2\pi \mathrm{i} \tau((k+2)x^2 - ky^2)}, \tag{31}$$

while the classical theta functions $\Theta_{m,k}(\tau)$ are defined as

$$\Theta_{n,m}(\tau, z, u) = \mathrm{e}^{-2\pi \mathrm{i} m u} \sum_{\ell \in \mathbb{Z} + (n/2m)} \mathrm{e}^{2\pi \mathrm{i} m \ell^2 \tau + 2\pi i \ell z}. \tag{32}$$

It follows from the coset construction that the essential ingredient in the conformal field theory is the SU(2) affine theory.

It was suggested by Gepner 15 years ago that exactly solvable string compactifications obtained by tensoring several copies of $N = 2$ minimal models should yield, after performing appropriate projections, theories that correspond in some limit to geometric compactification described by Brieskorn–Pham type Calabi–Yau varieties. The evidence for this conjecture was based initially mostly on spectral information for all models in the Gepner class of solvable string compactifications [32,33] and the agreement of certain types of intersection numbers which allow an interpretation as Yukawa couplings [34–37]. Alternative attempts to illuminate this surprising relation were based on Landau–Ginzburg theories [2–4] and

σ-models [5]. In the case of the Fermat cubic curve these results suggest that there is an underlying conformal field theory of this elliptic curve that is described by the GSO projection of a tensor product of three models at conformal level $k = 1$, as indicated in Section 1.

Given the fact that certain types of elliptic curves lead to modular forms, the question can be raised whether these forms are related, in some way, to the modular forms that arise from the conformal field theory. It is not clear a priori which of the field theoretic quantities should be the correct building blocks of the Hasse–Weil function, if any. What is clear is that none of the characters by themselves can be sufficient, perhaps via some polynomial expression, because their coefficients count multiplicities of the primary states. Both, the characters of the affine SU(2) theory

$$\chi^\ell(\tau, z, u) = \sum_{\substack{n=-k+1 \\ n=\ell \bmod 2}}^{k} c_n^\ell(\tau)\Theta_{n,k}(\tau, z, u), \tag{33}$$

as well as the characters of the parafermionic theory [38]

$$\kappa_m^\ell(\tau) = \eta(\tau)c_m^\ell(\tau), \tag{34}$$

which provides the intermediate step to $N = 2$ minimal models [39], could in principle play a role. In particular the string functions $c_m^\ell(\tau)$ of the $N = 2$ characters would appear to be natural candidates because they capture the essential interacting nature of the field theory. At conformal level $k = 1$ there is only one string function, which we denote by $c(\tau)$, and which can be computed to lead to the expansion

$$c(\tau) = q^{-1/24}(1 + q + 2q^2 + 3q^3 + 5q^4 + 7q^5 + \mathcal{O}(q^6)). \tag{35}$$

It turns out that more important than the string function itself is the associated SU(2) theta function

$$\Theta_m^\ell(\tau) = \eta^3(\tau)c_m^\ell(\tau). \tag{36}$$

At arbitrary level k these functions are Hecke indefinite modular forms associated to quadratic number fields determined by the level of the affine theory ([40] contains background material). At level $k = 1$ there is a unique theta function, which we denote by $\Theta(\tau)$, associated to the real quadratic extension $\mathbb{Q}(\sqrt{3})$ of the rational field $\mathbb{Q}$. Its expansion follows from the string function expansion, resulting in

$$\Theta(q) = q^{1/12}(1 - 2q - q^2 + 2q^3 + q^4 + 2q^5 + \mathcal{O}(q^6)). \tag{37}$$

This is a modular form of weight 1, which will emerge below as the building block of the Hasse–Weil modular form $f_{\mathrm{HW}}(C_3, q)$ of the cubic elliptic curve.

4. From geometry to modularity

The comparison of the modular forms encountered so far shows that there is no obvious relation between the geometric form $f_{\mathrm{HW}}(C_3, q)$ and the string function $c(q)$, or the associated theta function $\Theta(q)$ at (conformal) level 1. This is not surprising for a number

of reasons. The first is that characters of the conformal field theory by themselves are not useful because their coefficients count multiplicities, hence are always positive.

Secondly, we expect the prospective Hasse–Weil modular form of an elliptic curve to be of weight 2. This is neither the weight of the string function nor the weight of the theta function. The theta function $\Theta(\tau)$ is a form of weight 1, hence this problem could easily be fixed by considering a product of two such forms.

A further difference between the geometric and the conformal field theory forms is that the former have integral exponents, while the latter have rational exponents. Multiplying two theta functions together will in general not automatically fix this problem. The additional ingredient which serves as a useful guide is the concept of the conductor. For an elliptic curve this is a quantity which is determined both by the rational primes for which the reduced curve degenerates, i.e. the bad primes, as well as the degeneration type. Weil's important contribution to the Shimura–Taniyama conjecture was his recognition that this geometric conductor should determine the level of the modular form given by the L-function induced series.

In the case of the Fermat cubic curve the bad prime is given by $p = 3$. This means that the level of the prospective number theoretic modular form induced by the conformal field theory has to be divisible by 3. The conductor of the curve can be computed by first transforming the Fermat cubic into a Weierstrass form and then applying Tate's algorithm [41]. Since we are interested also in fields of characteristics 2 and 3, the usual (small) Weierstrass form $y^2 = 4x^3 + Ax + B$ is not appropriate. Instead, we have to consider the generalized Weierstrass form given by

$$E : y^2 + a_1xy + a_3y = x^3 + a_2x^2 + a_4x + a_6, \tag{38}$$

where the unusual index structure indicates the weight of the coefficients under admissible transformations which preserve this form

$$(x, y) \mapsto (u^2x + r, u^3y + u^2sx + t), \tag{39}$$

with $r, s, t \in K$ and $u \in K^*$ if E is defined over K. Curves of this type can acquire certain types of singularities when reduced over finite prime fields $\mathbb{F}_p$. The quantity which detects such singularities is the discriminant

$$\Delta = \frac{c_4^3 - c_6^2}{1728} \tag{40}$$

where

$$c_4 = b_2^2 - 24b_4, \qquad c_6 = -b_2^2 + 36b_2b_4 - 216b_6 \tag{41}$$

with

$$b_2 = a_1^2 + 4a_2, \qquad b_4 = a_1a_3 + 2a_4, \qquad b_6 = a_3^2 + 4a_6. \tag{42}$$

The curve E acquires singularities at those primes p for which $p|\Delta$. The singularity types that can appear have been classified by Kodaira and Néron [42], and are indicated by Kodaira's symbols. I_0 describes the smooth case, I_n $(n > 0)$ involve bad multiplicative reduction, and I_n^*, II, III, IV, II*, III*, IV* denote bad additive reduction.

The conductor itself depends on the detailed structure of the bad fiber and the discriminant. Conceptually, it is defined as an integral ideal of the field K over which the elliptic curve E is defined. By a result of Ogg [43] this ideal is determined by the number s_p of irreducible components of the singular fiber at p as well as the order $\mathrm{ord}_p \Delta_{E/K}$ of the discriminant $\Delta_{E/K}$ at p. In the present case the curve is defined over the field $K = \mathbb{Q}$, hence the ring of integers is a principal domain. The conductor can therefore be viewed as a number defined by

$$N_{E/\mathbb{Q}} = \prod_{\text{bad } p} p^{f_p}, \tag{43}$$

where the exponent f_p is given by

$$f_p = \mathrm{ord}_p \Delta_{E/\mathbb{Q}} + 1 - s_p. \tag{44}$$

The Fermat cubic can be transformed into a Weierstrass form by first choosing inhomogeneous coordinates and setting

$$\frac{x}{z} \mapsto -\frac{3u}{v}, \qquad \frac{y}{z} \mapsto \frac{9 - v}{v}. \tag{45}$$

This leads to the form $v^2 - 9v = u^3 - 27$. This result can be transformed further by completing the square and introducing the variables $x = u$ and $y = v - 5$, leading to the affine curve

$$y^2 + y = x^3 - 7 \tag{46}$$

with discriminant $\Delta = -3^9$ and j-invariant $j = 0$. The singular fiber resulting from Tate's algorithm is of Kodaira type IV* with $s_3 = 7$ components, leading to the conductor $N = 27$ (Fig. 1).

Combining the weight consideration with the integrality condition, as well as the conductor computation, suggests to look for modular forms of the type $\Theta(3a\tau)\Theta(3b\tau)$, where a, b are integers such that $(a + b) = 4$. This leads to the ansatz $f_1(\tau) = \Theta(3\tau)\Theta(9\tau)$ as a candidate modular form at conformal level $k = 1$. Expanding this form gives

$$\begin{aligned} f_1(\tau) = \Theta(3\tau)\Theta(9\tau) &= q - 2q^4 - q^7 + 5q^{13} + 4q^{16} - 7q^{19} \\ &\quad -5q^{25} + 2q^{28} - 4q^{31} + \cdots . \end{aligned} \tag{47}$$

Comparing this conformal field theoretic form with the form (21) shows complete agreement. This establishes a relation between the geometrically determined modular form

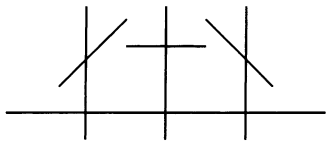

Fig. 1. The Kodaira type IV* type singularity, indicating the intersection properties.

derived from the Hasse–Weil L-function and a number theoretic modular form of the quadratic field $\mathbb{Q}(\sqrt{3})$ derived from an affine Kac–Moody algebra.

From the considerations of Section 2 we know that the form $f_1(\tau)$ is a normalized cusp Hecke eigenform of weight 2. In order to complete the identification of this form it is useful to recognize that the string function at conformal level one is given by the inverse of the Dedekind eta-function. Hence the theta function is given by the square of the η-function. This allows us to determine the (modular) level of the form by considering the level of the Fricke involution on the set of cusp forms of level N induced by the matrix

$$w_N = \begin{pmatrix} 0 & -1 \\ N & 0 \end{pmatrix}. \tag{48}$$

An eigenform f of weight 2 and level N transforms as

$$f\left(-\frac{1}{N\tau}\right) = \pm N\tau^2 f(\tau). \tag{49}$$

For the series $f_1(\tau)$ the Fricke involution leads to the result

$$f_1\left(-\frac{1}{27\tau}\right) = 27\tau^2 f_1(\tau). \tag{50}$$

Hence f_1 is a form at level 27, $f_1(\tau) = \Theta(3\tau)\Theta(9\tau) \in S_2(\Gamma_0(27))$.

This leaves the question whether there are other forms of this type. The dimension of $S_2(\Gamma_0(N))$ can be determined via the theory of modular curves $X_0(N)$ [10]. These are objects defined by quotients

$$X_0(N) = \mathfrak{H}^*/\Gamma_0(N), \tag{51}$$

where $\mathfrak{H}^* = \mathfrak{H} \cup \mathbb{Q} \cup \infty$ and $\mathfrak{H}$ is the upper half plane. Each form $f \in S_2(\Gamma_0(N))$ defines a differential form $\omega_f = 2\pi \mathrm{i} f(\tau)\,\mathrm{d}\tau$ on $X_0(N)$, hence the dimension of $S_2(\Gamma_0(N))$ is given by the genus of the curve

$$\dim S_2(\Gamma_0(N)) = g(X_0(N)). \tag{52}$$

The latter is determined completely by the index $\mu(N)$ of $\Gamma_0(N)$ in $\Gamma(1) = \mathrm{SL}(2,\mathbb{Z})$, its number of elliptic points of orders 2 and 3, $\nu_2(N)$ and $\nu_3(N)$, and the number of $\Gamma_0(N)$ inequivalent cusps $\nu_\infty(N)$. One has the following result.

Theorem (Shimura [10]). *The genus of $X_0(N)$ is given by*

$$g(X_0(N)) = 1 + \tfrac{1}{12}\mu(N) - \tfrac{1}{2}\nu_2(N) - \tfrac{1}{2}\nu_3(N) - \tfrac{1}{2}\nu_\infty. \tag{53}$$

Here the index is given by

$$\mu(N) = [\Gamma(1) : \Gamma_0(N)] = N \prod_{p|N} \left(1 + \frac{1}{p}\right), \tag{54}$$

while the number of elliptic points of order 2 *and* 3 *are given by*

$$\nu_2(N) = \left\{ \begin{array}{cc} 0 & \text{if } N \text{ is divisible by } 4 \\ \prod_{p|N}\left(1+\left(\frac{-1}{p}\right)\right) & \text{otherwise} \end{array} \right\},$$
$$\nu_3(N) = \left\{ \begin{array}{cc} 0 & \text{if } N \text{ is divisible by } 9 \\ \prod_{p|N}\left(1+\left(\frac{-3}{p}\right)\right) & \text{otherwise} \end{array} \right\}, \tag{55}$$

where the symbol $(\cdot/p)$ *denotes the quadratic residue symbol defined as*

$$\left(\frac{-1}{p}\right) = \left\{ \begin{array}{cc} 0 & \text{if } p = 2 \\ 1 & \text{if } p \equiv 1 \bmod 4 \\ -1 & \text{if } p \equiv 3 \bmod 4 \end{array} \right\}, \qquad \left(\frac{-3}{p}\right) = \left\{ \begin{array}{cc} 0 & \text{if } p = 3 \\ 1 & \text{if } p \equiv 1 \bmod 3 \\ -1 & \text{if } p \equiv 2 \bmod 3 \end{array} \right\}. \tag{56}$$

The number of cusps is given by

$$\nu_\infty^0(N) = \sum_{0<d|N} \phi\left(d, \frac{N}{d}\right). \tag{57}$$

Here $(d, N/d)$ *denotes the greatest common divisor and* $\phi(n)$ *is the Euler totient function.*

Computing the genus of the curve $X_0(27)$ then shows that the space $S_2(\Gamma_0(27))$ is one-dimensional, and that the form $f_1(\tau)$ is the unique generator (up to constants).

A priori these two series could be different at higher than computed order but, as mentioned before, general results by Faltings and Serre show that modular forms which agree to a sufficiently high, but finite, order, actually coincide. For modular forms of congruence groups $\Gamma_0(N)$ there is an explicit result which determines the congruence in a simple way [44]. For the situation of relevance here, this can be formulated as follows.

Theorem (Sturm). *Let* $f = \sum_n a_n q^n$ *and* $g = \sum_n b_n q^n$ *be modular forms of weight* k *with coefficients in the ring of integers* $\mathcal{O}_K$ *of some number field* K. *For prime ideals* $\mathfrak{p} \subset \mathcal{O}_K$ *and forms* f *define*

$$\mathrm{ord}_\mathfrak{p}(f) = \inf\{n | \mathfrak{p} \not| a_n\}. \tag{58}$$

Then, if

$$\mathrm{ord}_\mathfrak{p}(f-g) > \tfrac{1}{12} k[\Gamma_0(1) : \Gamma_0(N)] \tag{59}$$

one finds that $\mathrm{ord}_\mathfrak{p}(f-g) = \infty$, *i.e.* $\mathfrak{p} | (a_n - b_n)$ *for all* n.

This completes the proof of the theorem formulated in Section 1.

In the present case of elliptic curves constructive information is available in the form of the Eichler–Shimura theory. The following section describes how this framework fits into the general scheme of a conformal field theoric analysis of geometric compactifications via arithmetic methods.

5. From conformal field theory to geometry

Perhaps the most important problem in the context of string compactification is to invert the analysis described in the previous sections, and to ask how to construct a geometric target space from the data provided by the conformal field theory. This section describes the first steps in this direction. Our focus will mostly be on elliptic curves. This does not mean that these considerations are irrelevant for higher dimensional varieties. Examples where elliptic curves span part of the cohomology are threefolds such as transverse hypersurfaces of degree 12 embedded in $\mathbb{P}_{(1,1,2,4,4)}$. Here the singular set is given by the torus $C_3 \subset \mathbb{P}_2$ and its resolution contributes to the spectrum of the threefold. This resolution itself is determined in part by the cohomology of the curve C_3 and therefore the arithmetic of the elliptic curve becomes part of the arithmetic structure of the variety.

Conformal field theories can more usefully be thought of as determining pieces of cohomology, or more precisely, the motivic structure of the variety. Specifying the target motive is part of the external data that needs to be supplied to the conformal field theory. In the previous sections we have seen that, starting from a variety, it is possible to construct functions on the upper half plane that exhibit modular behavior, at least sometimes. In the case of elliptic curves over the rationals this has now been shown to always be the case, confirming Taniyama's intuition beyond his own expectations.

It is an open question at present which modular forms, or more generally, automorphic forms, are induced by motives. The structure that has emerged from the analysis of the congruent zeta function shows that a relation between modular forms and geometric objects very likely can be established only by considering certain subclasses of forms: (1) the form $f = \sum_n a_n q^n$ should be a cusp form, i.e. $a_0 = 0$; (2) f should be normalized, i.e. $a_1 = 1$; (3) f should be modular at some level N and (4) the form f should be a Hecke eigenform.

The expectation that these properties might suffice to guarantee a geometric origin of a modular form is suggested by the analysis of Atkin and Lehner. Denote the set of cusp forms of weight k and level N by $S_k(\Gamma_0(N))$, and define a newform as an element in this space that is not determined by a level N' that is a divisor of N.

Theorem (Atkin–Lehner). *Let $S_k(\Gamma_0(N)) \ni f = \sum_{n=1}^{\infty} a_n q^n$ be a normalized cusp form which is a newform and is an eigenvector for all Hecke operators $T_k(n)$. Then*

$$L(f,s) = \prod_{\substack{p \text{ prime} \\ p|N,\, p^2 \nmid N}} \frac{1}{1+\lambda(p)p^{(k/2)-1-s}} \prod_{\substack{p \text{ prime} \\ p \nmid N}} \frac{1}{1-a_p p^{-s}+p^{k-1-2s}}, \tag{60}$$

where $\lambda(p) = \pm 1$.

Comparing this result with the definition of the Hasse–Weil L-series shows that it is this class of modular forms which admits a possible geometric interpretation.

The strategy adopted here to go from such modular forms to geometry is based on results by Eichler and Shimura [45,46]. Given a cusp Hecke eigenform f of weight 2 and level N the Eichler–Shimura construction leads to an abelian variety A_f whose dimension is

determined by the degree of the field extension $K = \mathbb{Q}(\{a_n\})$ defined by the coefficients of the modular form [47]

$$\dim_{\mathbb{C}} A_f = [K : \mathbb{Q}]. \tag{61}$$

The importance of A_f derives from the fact that its arithmetic properties are determined by the modular form in the sense that the Mellin transform of its Hasse–Weil L-function $L(A_f, s)$ is determined by the L-series of the modular form f. In more detail, the concrete construction of A_f proceeds by recovering it as a factor in the Jacobian of the modular curve $X_0(N)$ defined as the compactification of the affine curve

$$Y_0(N) = \mathfrak{H}/\Gamma_0(N), \tag{62}$$

where $\mathfrak{H}$ is the upper half plane.

Intuitively, this abelian factor can be viewed as the subvariety, or factor, of the Jacobian of the modular curve spanned by the set $\{f^\sigma\}$ of conjugate forms obtained from the set $\{\sigma : K \to \mathbb{C}\}$ of embeddings of the coefficient field K. Associated to a modular form f of weight 2 and level N on the upper half plane $\mathfrak{H}$ is a holomorphic differential $\omega_f = 2\pi \mathrm{i} f(z)\, \mathrm{d}z$, which descends to the quotient Riemann surface $\mathfrak{H}/\Gamma_0(N)$ and extends to the compactification $X_0(N)$ over $\mathbb{Q}$, defining a 1-form ω_f on the modular curve $X_0(N)$.

If f has rational coefficients then (61) shows that the abelian variety is an elliptic curve E. The results of Eichler and Shimura can further be used to establish that the Hasse–Weil L-function $L(E, s)$ associated to f agrees with the L-series of f for almost all primes. The construction of Eichler–Shimura provides a map

$$\Phi_f : \Gamma_0(N) \to \mathbb{C} \tag{63}$$

that annihilates the elliptic and parabolic points. If f is not only a newform but also a Hecke eigenform such that the Hecke eigenvalues are integers then Φ_f determines a lattice and the resulting elliptic curve E, the modular curve $X_0(N)$, and the map

$$X_0(N) \to E \tag{64}$$

are defined over $\mathbb{Q}$. Igusa [48] improved this result by showing that the only possible exception are the bad primes dividing the level N. It was finally shown by Carayol that indeed the arithmetic agreement holds for all primes and therefore one finally has the following result.

Theorem (Carayol [49]). *Let $f \in S_2(\Gamma_0(N))$ be a normalized newform with integral coefficients in $\mathbb{Z}$ and let E be the elliptic curve associated to f via the Eichler–Shimura construction. Then*

$$L(E, s) = L(f, s) \tag{65}$$

and N is the conductor of E.

It is not obvious that the curve E obtained in this way should have the same arithmetic as the Fermat curve which was the starting point of the considerations above. It turns out, however, that both the Fermat curve C_3 and the abelian variety A_f are on equal footing as far

as their arithmetic properties are concerned. The concept that captures what might be called the 'arithmetic equivalence' of elliptic curves, and more generally of abelian varieties, is that of an isogeny. A non-constant analytic map $E \to E'$ between two elliptic curves E and E' is called an isogeny if it takes the distinguished point O of E, given by the zero of the algebraic group structure, into the corresponding point O' of E'. If such a map exists then E and E' are said to be isogenous. Two isogenous elliptic curves over $\mathbb{Q}$ have the same primes of bad reduction [50], and furthermore for each good prime their cardinalities agree, $\#(E/\mathbb{F}_p) = \#(E'/\mathbb{F}_p)$. An important result by Faltings, proving a conjecture of Tate, shows that the converse holds.

Theorem (Tate, Faltings [51]). *Two elliptic curves E, E' over the rational field $\mathbb{Q}$ which have the same L-function are isogenous.*

These results indicate that in the context of trying to understand conformal field theoretical aspects of string compactifications via the arithmetic structure of the varieties we should not consider individual varieties as objects corresponding to the conformal field theory. Instead, it is more useful to think in terms of equivalence classes of varieties, where the equivalence relation is given by the concept of isogeny.

6. Representation theoretic framework

There is an alternative framework which provides a tool to analyze the arithmetic structure of algebraic varieties, and which allows to think somewhat differently about the deeper issues involved in the relation between Calabi–Yau varieties and affine Kac–Moody algebras. This formulation involves representations of the absolute Galois group $\mathrm{Gal}(\bar{\mathbb{Q}}/\mathbb{Q})$, defined as the group of automorphisms of the algebraic closure $\bar{\mathbb{Q}}$ of the rational field that leaves $\mathbb{Q}$ fixed, and therefore relates to a question raised in [52]. Moore observed that the Galois group of the class field $\hat{K}$ of a field K acts on the vector multiplet attractor moduli and asked whether the absolute Galois group $\mathrm{Gal}(\bar{\mathbb{Q}}/\mathbb{Q})$ plays a role in some compactifications. The following considerations show such an application in a physical context.

The group $\mathrm{Gal}(\bar{\mathbb{Q}}/\mathbb{Q})$ can be viewed as a limit of the Galois groups $\mathrm{Gal}(K/\mathbb{Q})$ where K runs through all possible finite extensions of $\mathbb{Q}$ in $\bar{\mathbb{Q}}$. Any element of $\mathrm{Gal}(\bar{\mathbb{Q}}/\mathbb{Q})$ determines a system σ of automorphisms σ_K in each of the individual Galois groups $\mathrm{Gal}(K/\mathbb{Q})$. The σ_K are compatible in the sense that if one has two extensions K, L of $\mathbb{Q}$ such that $K \subset L$ then the automorphisms $\sigma_K \in \mathrm{Gal}(K/\mathbb{Q})$ and $\sigma_L \in \mathrm{Gal}(L/\mathbb{Q})$ are such that σ_L restricts to σ_K, i.e. $\sigma_K = \sigma_L|_K$.

The goal in number theory is to understand the absolute Galois group $\mathrm{Gal}(\bar{\mathbb{Q}}/\mathbb{Q})$ via its n-dimensional continuous representations

$$\rho : \mathrm{Gal}(\mathbb{Q}/\mathbb{Q}) \to \mathrm{GL}(n, K), \tag{66}$$

where K is a (topological) field which can, e.g. be the complex field $\mathbb{C}$, the p-adic field $\mathbb{Q}_p$ or some extension of it, or it can be some finite field. The latter case turns out to be of interest in the present context.

For any elliptic curve E representations of the absolute Galois group can be constructed from the group $E[n]$ of torsion points, i.e. the subgroup of points of the group $E(\bar{\mathbb{Q}})$ for which $nx = 0$. The underlying group operation is written additively, $P_1 + P_2$, where the sum of two points is defined as the intersection point of the line connecting the points P_1, P_2 with the elliptic curve (see e.g. [53]). If the curve is described by the generalized Weierstrass form (38), the line $y = mx + b$ connecting two points $P_1 = (x_1, y_1)$ and $P_2 = (x_2, y_2)$ is determined by

$$m = \left\{ \begin{array}{ll} \dfrac{y_2 - y_1}{x_2 - x_1} & \text{if } P_1 \neq P_2 \\ \dfrac{3x_1^2 + 2a_2x_1 + a_4 - a_1y_1}{2y_1 + a_1x_1 + a_3} & \text{if } P_1 = P_2 \end{array} \right\} \tag{67}$$

and

$$b = \left\{ \begin{array}{ll} \dfrac{y_1x_2 - y_2x_1}{x_2 - x_1} & \text{if } P_1 \neq P_2 \\ \dfrac{-x_1^3 + a_4x_1 + 2a_6 - a_3y_1}{2y_1 + a_1x_1 + a_3} & \text{if } P_1 = P_2 \end{array} \right\}. \tag{68}$$

The intersection point $P_3 = (x_3, y_3)$ of the line with the curve is then given by

$$x_3 = m^2 + a_1m - a_2 - x_1 - x_2, \qquad y_3 = -(m + a_1)x_3 - b - a_3 \tag{69}$$

in both the chord case ($P_1 \neq P_2$) and the tangent case ($P_1 = P_2$).

The group $E[n]$ of points of order n is a free $\mathbb{Z}/n\mathbb{Z}$-module of rank 2, i.e. $E[n] \cong \mathbb{Z}/n\mathbb{Z} \times \mathbb{Z}/n\mathbb{Z}$. It is possible to define an action of the absolute Galois group on $E[n]$ via a homomorphism

$$\rho_n : \mathrm{Gal}(\bar{\mathbb{Q}}/\mathbb{Q}) \to \mathrm{Aut}(E[n]) \cong \mathrm{GL}(2, \mathbb{Z}/n\mathbb{Z}). \tag{70}$$

The image $\rho_n(\mathrm{Gal}(\bar{\mathbb{Q}}/\mathbb{Q}))$ in $\mathrm{GL}(2, \mathbb{Z}/n\mathbb{Z})$ can be thought of as the Galois group $\mathrm{Gal}(K[n]/\mathbb{Q})$ of the field extension $K[n]$ obtained by adjoining the coordinates of the points of $E[n]$ to the rationals. More precisely, one has the following.

Theorem (Serre [54]). *The x and y coordinates of the points of $E[n]$ have algebraic values. If $K[n]$ is the field extension obtained from $\mathbb{Q}$ by adjoining all coordinates of these points then $K[n]$ is a Galois extension and the representation ρ_n factors through* $\mathrm{Gal}(\bar{\mathbb{Q}}/\mathbb{Q})$, *i.e.*

$$\mathrm{Gal}(\bar{\mathbb{Q}}/\mathbb{Q}) \to \mathrm{Gal}(K[n]/\mathbb{Q}) \to \mathrm{GL}(2, \mathbb{Z}/n\mathbb{Z}), \tag{71}$$

where the map on the left is the canonical surjection and the map on the right is injective.

The interesting aspect of these representations is that they can be related to the arithmetic of the variety discussed in previous sections. Roughly, this can be outlined as follows. From the normal extension $K[n]/\mathbb{Q}$ one obtains a map

$$\rho : \mathrm{Gal}(K[n]/\mathbb{Q}) \to \mathrm{GL}(2, \mathbb{Z}/n\mathbb{Z}). \tag{72}$$

The subfield of $K[n]$ whose Galois group is $\rho^{-1}(\mathrm{SL}(2,\mathbb{Z}/n\mathbb{Z})) \subset \mathrm{Gal}(K[n]/\mathbb{Q})$ is the cyclotomic field $\mathbb{Q}(\mu_n)$. The basic idea is to associate to a rational prime p a class of conjugate elements $\sigma_{\mathfrak{p}}$ in $\mathrm{Gal}(K[n]/\mathbb{Q})$ and to analyze its characteristic polynomial. Consider a rational prime p which is different from n and the conductor N, and therefore unramified in $K[n]$, i.e. every prime ideal $\mathfrak{p}_i$ appears with multiplicity one in the decomposition of p. Let $\mathfrak{p}$ be a prime ideal in $K[n]$ which divides the principal ideal (p). Associated to these two ideals is the field extension $\mathbb{F}_{\mathrm{N}\mathfrak{p}}/\mathbb{F}_p$, defined by the residue fields $\mathbb{F}_{\mathrm{N}\mathfrak{p}} = \mathcal{O}_{K[n]}/\mathfrak{p}$ and $\mathbb{F}_p = \mathbb{Z}/(p)$. Here $\mathrm{N}\mathfrak{p}$ denotes the norm of the ideal $\mathfrak{p}$, defined conceptually as the cardinality of the resulting residue field. In the present context we are interested in Galois extensions and the norm of a prime ideal can be computed most easily by considering the Galois conjugates of the ideal

$$\mathrm{N}\mathfrak{p} = \prod_{\sigma\in\mathrm{Gal}(K[n]/\mathbb{Q})} \sigma(\mathfrak{p}). \tag{73}$$

The Galois group of the finite extension $\mathbb{F}_{\mathrm{N}\mathfrak{p}}$ is particularly simple in that it is a cyclic group whose generator is given by the Frobenius automorphism $x \mapsto x^p$. Furthermore, there is a surjective map from the decomposition group, defined by

$$D_{\mathfrak{p}} = \{\sigma \in \mathrm{Gal}(K[n]/\mathbb{Q}) | \sigma(\mathfrak{p}) = \mathfrak{p}\} \tag{74}$$

onto this Galois group

$$D_{\mathfrak{p}} \to \mathrm{Gal}(\mathbb{F}_{\mathrm{N}\mathfrak{p}}/\mathbb{F}_p). \tag{75}$$

The element $\sigma_{\mathfrak{p}}$ is defined as that element in the decomposition group which corresponds to this generator of the cyclic Galois group. Given the Frobenius automorphism of $K[n]/\mathbb{Q}$ associated to $\mathfrak{p}$ one obtains the following congruence:

$$\det(t\cdot\mathbf{1} - \rho(\sigma_{\mathfrak{p}})) = t^2 - c_p t + p \bmod n, \tag{76}$$

where t is a formal variable and the coefficient c_p is a rational integer.

The connection with the arithmetic consideration is made by the observation that the coefficients c_p are determined by the cardinalities of the curve. Results of this type are described in [55]. It might appear that the Galois representations contain only reduced information about the arithmetic of the variety because of the mod condition in (76). Surprisingly this is not the case if one considers not only representations at any fixed prime ℓ but combines the representations associated to $E[\ell^n]$, $n \in \mathbb{N}$, into a so-called ℓ-adic representation ρ_{ℓ^∞} of the absolute Galois group $\rho_{\ell^\infty} : \mathrm{Gal}(\bar{\mathbb{Q}}/\mathbb{Q}) \to \mathrm{GL}(2,\mathbb{Z}_\ell)$, where $\mathbb{Z}_\ell$ denotes the ℓ-adic integers. Then one has the following result.

Theorem (Serre [54]). *Each ℓ-adic representation determines the curve E up to isogeny.*

The Galois theoretic framework suggests that an alternative way of thinking about the reconstruction of spacetime from the string is to ask what the Galois representations are that are induced by the conformal field theory and how they are related to those that are induced by the structure of spacetime. A number of results about Galois representations that are either known or conjectured are of relevance in this context.

It turns out that the mathematically easier direction is the one that has been the more challenging from a physics perspective and involves the problem of constructing spacetime from string theory. Starting from a Hecke cusp eigenform f of weight k constructed from a conformal field theory, results from Shimura, Deligne, and Deligne–Serre show that there exists a continuous representation

$$\rho_f : \mathrm{Gal}(\bar{\mathbb{Q}}/\mathbb{Q}) \to \mathrm{GL}(2, \bar{\mathbb{F}}_\ell) \tag{77}$$

such that

$$\mathrm{tr}\, \rho_f(\sigma_p) = a_p (\mathrm{mod}\, \ell), \qquad \det \rho_f(\sigma_p) = \epsilon(p) p^{k-1} (\mathrm{mod}\, \ell), \tag{78}$$

where p runs through the rational primes not dividing ℓ and $\sigma_p \in \mathrm{Gal}(\bar{\mathbb{Q}}/\mathbb{Q})$ is the Frobenius automorphism corresponding to any prime ideal $\mathfrak{p}$ of $\bar{\mathbb{Z}}$ lying over p. $\bar{\mathbb{F}}_\ell$ is the algebraic closure of the finite field $\mathbb{F}_\ell$ and $\epsilon : (\mathbb{Z}/N\mathbb{Z})^\times \to \mathbb{C}^\times$ is the character induced by the diamond bracket operator (see e.g. [56]). For modular forms of higher weight k the construction is involved, but for the simpler case $k = 2$, which is of relevance for the present context, the Galois representation can be obtained via the Eichler–Shimura theory described above. It emerges as the action of $\mathrm{Gal}(\bar{\mathbb{Q}}/\mathbb{Q})$ on the torsion points obtained from an elliptic 'piece' of the modular curve $X_0(N)$. More precisely, one combines all the torsion points into the Tate module, an infinite tower of compatible torsion point groups on which the Galois group acts.

Once we have a Galois representation, derived from the conformal field theory, we can ask what the underlying geometry is of such representations, if any. This line of thought is useful because a result of Faltings [51] shows that abelian varieties are uniquely determined up to isogeny by their Galois representations. This means that the arithmetic properties of abelian varieties are determined by their Galois representation and explains why the concept of modularity can be recovered in this context. Work in this direction is based mostly on conjectures by Fontaine and Mazur [57].

Fewer results are available in the direction which passes from the geometry to modularity via the Galois group, because the transition from Galois representations to modular forms is based on conjectures by Serre which have yet to be proven. Suppose we start from a geometrically induced continuous irreducible representation $\rho : \mathrm{Gal}(\bar{\mathbb{Q}}/\mathbb{Q}) \to \mathrm{GL}(2, \mathbb{F}_\ell)$ with odd determinant, i.e. $\det \rho(\sigma_\infty) = -1$, where $\sigma_\infty \in \mathrm{Gal}(\bar{\mathbb{Q}}/\mathbb{Q})$ is the restriction to $\bar{\mathbb{Q}}$ of complex conjugation in $\mathbb{C}$. Then Serre's conjecture states that such a Galois representation is induced by a modular form and it provides a prescription for computing the modular level N, the weight k, and the character ϵ for which the eigenform f should exist. A review of the status of the Serre conjectures can be found in [56].

Acknowledgements

It is a pleasure to thank Monika Lynker and John Stroyls for discussions. Part of this work was completed while RS was supported as a Scholar at the Kavli Institute for Theoretical Physics in Santa Barbara. It is a pleasure to thank the KITP and Indiana University at South Bend for hospitality. This work was supported in part by the National Science Foundation under Grant No. PHY99-07949.

References

[1] R. Schimmrigk, Arithmetic of Calabi–Yau varieties and rational conformal field theory, J. Geom. Phys. 44 (2002) 555–569. arXiv: hep-th/0111226.
[2] E. Martinec, Algebraic geometry and effective Lagrangians, Phys. Lett. B 217 (1989) 431.
[3] N. Warner, C. Vafa, Catastrophes and the classification of conformal theories, Phys. Lett. B 218 (1989) 51.
[4] W. Lerche, N. Warner, C. Vafa, Chiral rings in $N = 2$ superconformal theories, Nucl. Phys. B 324 (1989) 427.
[5] E. Witten, Phases of $N = 2$ theories in 2 dimensions, Nucl. Phys. B 403 (1993) 159–222. arXiv: hep-th/9301042.
[6] G. Shimura, Yutaka Taniyama and his time, Bull. Lond. Math. Soc. 21 (1989) 186–196.
[7] G. Shimura, On elliptic curves with complex multiplication as factors of Jacobian varieties, Nagoya Math. J. 43 (1971) 199–208.
[8] A. Weil, Über die Bestimmung Dirichletscher Reihen durch Funktionalgleichungen, Math. Ann. 168 (1967) 149–156.
[9] S. Lang, Some history of the Shimura–Taniyama conjecture, Notices AMS 42 (1995) 1301–1307.
[10] G. Shimura, Introduction to the Arithmetic Theory of Automorphic Forms, Princeton, 1971.
[11] G. Frey, Links between stable elliptic curves and certain diophantine equations, Ann. Univ. Sarav. Ser. Math. 1 (1986) 1–40.
[12] K. Ribet, On modular representations of $\mathrm{Gal}(\bar{\mathbb{Q}}/\mathbb{Q})$ arising from modular forms, Invent. Math. 100 (1990) 431–476.
[13] A. Wiles, Modular elliptic curves and Fermat's last theorem, Ann. Math. 141 (1995) 443–551.
[14] R. Taylor, A. Wiles, Ring-theoretic properties of certain Hecke algebras, Ann. Math. 141 (1995) 553–572.
[15] F. Diamond, On deformation rings and Hecke rings, Ann. Math. 144 (1996) 137–166.
[16] B. Conrad, F. Diamond, R. Taylor, Modularity of certain potentially Barsotti–Tate Galois representations, J. Am. Math. Soc. 12 (1999) 521–567.
[17] C. Breuil, B. Conrad, F. Diamond, R. Taylor, On the modularity of elliptic curves over $\mathbb{Q}$ or Wild 3-adic exercises, J. Am. Math. Soc. 14 (2001) 843–939.
[18] D. Gepner, Spacetime supersymmetry in compactified string theory and superconformal models, Nucl. Phys. B 296 (1988) 757.
[19] S. Gukov, C. Vafa, Rational conformal field theory and complex multiplication. arXiv: hep-th/0203213.
[20] H. Hasse, Zetafunktion und L-funktionen zu einem arithmetischen funktionenkörper vom fermatschen typus, Abh. d. Deutschen Akad. d. Wiss. Berlin, Math.-Nat. Kl. 1954, pp. 5–70.
[21] A. Weil, Number theory and algebraic geometry, in: Proceedings of the International Congress on Mathematics, American Mathematical Society, Providence, RI, 1950.
[22] A. Weil, Jacobi sums as Grössencharaktere, Trans. Am. Math. Soc. 73 (1952) 487–495.
[23] A. Weil, Number of solutions of equations in finite fields, Bull. Am. Math. Soc. 55 (1949) 497.
[24] E. Artin, Quadratische Körper im Gebiete der früheren Kongruenzen I, II, Math. Z. 19 (1924) 153–216.
[25] F.K. Schmidt, Zur Zahlentheorie in Körpern der Charakteristik p (Vorläufige Mitteilung), Sitz.-Ber. Phys. Med. Soz. Erlangen 58/59 (1926/1927) 159–172.
[26] F.K. Schmidt, Analytische Zahlentheorie in Körpern der Charakteristik p, Math. Z. 33 (1931) 1–32.
[27] H. Hasse, Beweis des Analogons der Riemannschen Vermutung für die Artinschen und F.K. Schmidtschen Kongruenzzetafunktionen in gewissen elliptischen Fällen. Vorläufige Mitteilung, Nachrichten v.d. Gesellschaft d. Wiss. zu Göttingen I. Nr. 42, 1933, pp. 253–262.
[28] H. Hasse, Über die Kongruenzzetafunktionen. Unter Benutzung von Mitteilungen von Prof. Dr. F.K. Schmidt und Prof. Dr. E. Artin, S. Ber. Preuß. Akad. Wiss. H. 17 (1934) 250–263.
[29] P. Roquette, Zur Geschichte der Zahlentheorie in den dreiß iger Jahren, Jahrbuch 1996 der Braunschweigischen Wissenschaftlichen Geselllschaft, 1997.
[30] J.-P. Serre, Zeta and L-functions, arithmetical algebraic geometry, in: Proceedings of the Conference, Purdue, 1965.
[31] A.O.L. Atkin, J. Lehner, Hecke operators on $\Gamma_0(m)$, Math. Ann. 185 (1970) 134–160.
[32] M. Lynker, R. Schimmrigk, A–D–E quantum Calabi–Yau manifolds, Nucl. Phys. B 339 (1990) 121–157.
[33] J. Fuchs, A. Klemm, C. Scheich, M.G. Schmidt, Spectra and symmetries of Gepner models compared to Calabi–Yau compactifications, Ann. Phys. 204 (1990) 1–51.

[34] B.R. Greene, K.H. Kirklin, P.J. Miron, G.G. Ross, 27^3 Yukawa couplings for a three generation superstring model, Phys. Lett. B 192 (1987) 111.
[35] J. Distler, B.R. Greene, K. Kirklin, P. Miron, Evaluation of 27-Bar**3 Yukawa couplings in a three generation superstring model, Phys. Lett. B 195 (1987) 41.
[36] G. Sotkov, M. Stanishkov, Yukawa couplings for the three generation string model, Phys. Lett. B 215 (1988) 674.
[37] R. Schimmrigk, Heterotic (2,2) vacua: manifold theory and exact results, Nucl. Phys. B 342 (1990) 231–245.
[38] A.B. Zamolodchikov, V.A. Fateev, Nonlocal (parafermion) currents in two-dimensional conformal quantum field theory and self-dual critical points in $\mathbb{Z}(N)$ systems, Sov. Phys. JETP 62 (1985) 215.
[39] A.B. Zamolodchikov, V.A. Fateev, Disorder fields in two-dimensional conformal quantum field theory and $N = 2$ extended supersymmetry, Zh. Eksp. Theor. Fiz. 90 (1986) 1553.
[40] V.G. Kac, D.H. Peterson, Infinite-dimensional lie algebras, theta functions and modular forms, Adv. Math. 53 (1984) 125–264.
[41] J. Tate, Algorithm for determining the type of a singular fiber in on elliptic pencil, Letter to J. Cassels, in: B.J. Birch, W. Kuyk (Eds.), Modular Functions of One Variable IV, LNM 476, Springer, Berlin, 1975.
[42] A. Néron, Modèles minimaux des variétés abéliennes sur les corp loceaux et globeaux, IHES Publ. Math. 21 (1964) 361–482.
[43] A. Ogg, Elliptic curves and wild ramifications, Am. J. Math. 89 (1967) 1–21.
[44] J. Sturm, On the congruence of modular forms, in: D.V. Chudnovsky, G.V. Chudnovsky, H. Cohn, M.B. Nathanson (Eds.), Number Theory, LNM 1240, Springer, Berlin, 1987.
[45] M. Eichler, Quaternäre quadratische Formen und die Riemannsche Vermutung für die Kongruenzzeta-funktion, Arch. Math. 5 (1954) 355–366.
[46] G. Shimura, Correspondences modulaires et les fonction ζ de courbes algebrique, J. Math. Soc. Jpn. 10 (1958) 1–28.
[47] G. Shimura, Sur les intégrales attachés aux formes automorphes, J. Math. Soc. Jpn. 11 (1959) 291–311.
[48] J. Igusa, Kroneckerian models of fields of elliptic modular functions, Am. J. Math. 81 (1959) 561–577.
[49] H. Carayol, Sur les représentation ℓ-adiques associées aux formes modulaires de Hilbert, Ann. Scient. École Norm. Sup. 19 (1986) 409–468.
[50] J.-P. Serre, J. Tate, Good reduction of abelian varities, Ann. Math. 88 (1968) 492–517.
[51] G. Faltings, Endlichkeitssätze für abelsche Varietäten über Zahlkörpern, Invent. Math. 73 (1983) 349–366.
[52] G. Moore, Attractors and arithmetic. arXiv: hep-th/9807056; Arithmetic and attractors. arXiv: hep-th/9807087.
[53] A.W. Knapp, Elliptic Curves, Princeton Univ. Press, Princeton, 1992.
[54] J.-P. Serre, Abelian ℓ-adic Representations and Elliptic Curves, Benjamin, 1968.
[55] G. Shimura, A reciprocity law in non-solvable extensions, J. Reine Angew. Math. 221 (1966) 209–220.
[56] K. Ribet, W. Stein, Introduction to Serre's conjectures, in: B. Conrad (Ed.), Arithmetic Algebraic Geometry, AMS, Providence, RI, 2000.
[57] J.-M. Fontaine, B. Mazur, Geometric Galois representations, in: J. Coates, S.-T. Yau (Eds.), Elliptic Curves, Modular Forms, and Fermat's Last Theorem, International Press, 1995.