THE SHIMURA-TANIYAMA CONJECTURE - Also referred to in the literature as the Shimura-Taniyama-Weil conjecture, the Taniyama-Shimura conjecture, the Taniyama-Weil conjecture, or the modularity conjecture, it postulates a deep connection between **elliptic curves** over the rational numbers and **modular forms**. It has now been almost completely proved thanks to the fundamental work of A. Wiles and R. Taylor [W], [TW], and its further refinements [Di], [CDT].

Let $\Gamma_0(N)$ be the group of matrices in $\mathbf{SL}_2(\mathbf{Z})$ which are upper triangular modulo a given positive integer N. It acts as a discrete group of **Mobius transformations** on the **Poincaré upper half-plane** $\mathcal{H} := \{z \in \mathbf{C} | Im(z) > 0\}$. A **cusp form** of weight 2 for $\Gamma_0(N)$ is an **analytic function** f on $\mathcal{H}$ satisfying the relation $f\left(\frac{az+b}{cz+d}\right) = (cz+d)^2 f(z), \quad$ for all $\begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \Gamma_0(N)$, together with suitable growth conditions on the boundary of $\mathcal{H}$. (Cf. **Modular forms**.) The function f is periodic of period 1, and it can be written as a **Fourier series** in $q = e^{2\pi i z}$ with no constant term: $f(z) = \sum_{n=1}^{\infty} \lambda_n q^n$. The **Dirichlet series** $L(f,s) = \sum \lambda_n n^{-s}$ is called the L-function attached to f. (Cf. L**-functions**.) It is essentially the **Mellin transform** of f: $\Lambda(f,s) := \Gamma(s)L(f,s) = (2\pi)^s \int_0^{\infty} f(iy) y^{s-1} dy$. The space of cusp forms of weight 2 on $\Gamma_0(N)$ is a finite-dimensional vector space and is preserved by the involution W_N defined by $W_N(f)(z) = Nz^2 f(\frac{-1}{Nz})$. Hecke showed that if f lies in one of the two eigenspaces for this involution (with eigenvalue $w = \pm 1$) then $L(f,s)$ satisfies the functional equation: $\Lambda(f,s) = -w\Lambda(f, 2-s)$, and that $L(f,s)$ has an analytic continuation to all of $\mathbf{C}$.

Let E be an **elliptic curve** over the rationals, and let $L(E,s)$ denote its **Hasse-Weil** L**-series**. The curve E is said to be **modular** if there exists a cusp form f of weight 2 on $\Gamma_0(N)$ for some N such that $L(E,s) = L(f,s)$. The Shimura-Taniyama conjecture asserts that every elliptic curve over $\mathbf{Q}$ is modular. Thus it gives a framework for proving the analytic continuation and functional equation for $L(E,s)$. It is prototypical of a general relationship between the L-functions attached to arithmetic objects and those attached to **automorphic forms**, as described in the far-reaching **Langlands program**.

Weil's refinement of the conjecture predicts that the integer N is equal to the **arithmetic conductor** of E. Thanks to the ideas introduced by

Wiles (cf. [CDT]) one now knows that E is modular, if 27 does not divide the conductor of E. Wiles' proof proceeds by viewing the Shimura-Taniyama conjecture in a wider framework which predicts the modularity of the (two-dimensional) **Galois representations** arising from the cohomology of varieties over $\mathbf{Q}$.

The modularity of E can also be formulated as the statement that E is a quotient of the **modular curve** $X_0(N)$ over $\mathbf{Q}$; this curve represents the solution to the moduli problem of classifying pairs (A, C) consisting of an elliptic curve A with a distinguished cyclic subgroup C of order N. Alternately, if E is modular, then there is a (non-constant) complex analytic uniformisation $\mathcal{H}/\Gamma_0(N) \longrightarrow E(\mathbf{C})$.

The importance of the Shimura-Taniyama conjecture is manifold. Firstly it gives the analytic continuation of $L(E, s)$ for a large class of elliptic curves. The L-function itself plays a key role in the study of E, most notably through the celebrated **Birch and Swinnerton-Dyer conjecture**. Secondly, the modular curve $X_0(N)$ is endowed with a natural collection of algebraic points arising from the theory of **complex multiplication**, and the existence of a modular parametrisation allows the construction of points on E defined over abelian extensions of certain imaginary quadratic fields. This fact was exploited by Gross-Zagier and Kolyvagin to give strong evidence for the **Birch and Swinnerton-Dyer conjecture** for E, under the assumption that E is modular.

The Shimura-Taniyama conjecture admits various generalizations. Replacing $\mathbf{Q}$ by an arbitrary number field K, it predicts that an elliptic curve E over K is associated to an **automorphic form** on $\mathbf{GL}_2(K)$. When K is totally real, such an E is often uniformized by a **Shimura curve** attached to a suitable **quaternion algebra** over K with exactly one split place at infinity (when K is of odd degree, or when E has at least one prime of multiplicative reduction.) In the context of **function fields** over finite fields, the Shimura-Taniyama conjecture admits an analogue which was established earlier by Drinfeld using methods different from those of Wiles.

References

[CDT] CONRAD, B., DIAMOND, F. AND TAYLOR, R.: 'Modularity of certain potentially Barsotti-Tate Galois representations'. *J. Amer.*

Math. Soc., to appear.

[Di] DIAMOND, F.: 'On deformation rings and Hecke rings'. *Ann. of Math.* (2) **144** (1996), no. 1, 137–166.

[TW] TAYLOR, R., AND WILES, A.: 'Ring-theoretic properties of certain Hecke algebras', *Annals of Mathematics.* (2) **141** (1995), no. 3, 553–572.

[W] WILES, A.: 'Modular elliptic curves and Fermat's last theorem'. *Annals of Mathematics.* (2) **141** (1995), no. 3, 443–551.

H. Darmon