An overview of the Taylor-Wiles Method

Sachin Kumar
University of Waterloo, Faculty of Mathematics

April 2023

Generalities

Let $\overline{\mathbb{Q}}$ be the algebraic closure of $\mathbb{Q}$ and $\text{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})$ is called the absolute Galois group of $\mathbb{Q}$. Given a number field L, $\text{Gal}(\overline{\mathbb{Q}}/L)$ is an open subgroup of $\text{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})$. As L ranges over all number fields, the groups $\text{Gal}(\overline{\mathbb{Q}}/L)$ consist of a basis of open neigbourhoods of the identity. Given a prime number p, the ring of p-adic integers is the inverse limit $\mathbb{Z}_p = \lim_{\longleftarrow} \mathbb{Z}/p^n\mathbb{Z}$ and let $\mathbb{Q}_p$ be the fraction field of $\mathbb{Z}_p$.

Galois Representation

Let V be a finite dimensional $\mathbb{Q}_p$-vector space equipped with a continuous action of $\text{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})$. This gives rise to a continuous Galois representation, $\rho_V : \text{Gal}(\overline{\mathbb{Q}}/\mathbb{Q}) \to GL_n(\mathbb{Q}_p)$. Here, $GL_n(\mathbb{Q}_p)$ is the automorphism group of $V \simeq \mathbb{Q}_p^n$. There is a $\mathbb{Z}_p$-linear lattice $L \simeq \mathbb{Z}_p^n$ contained in V which is Galois stable. The action of $\text{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})$ gives rise to an integral Galois representation, $\rho : \text{Gal}(\overline{\mathbb{Q}}/\mathbb{Q}) \to GL_n(\mathbb{Z}_p)$. Let E be an elliptic curve defined over $\mathbb{Q}$ and p be a prime number. Given $N \in \mathbb{Z}_{\geq 1}$, set $E[n]$ to denote the N-torsion subgroup of $E(\overline{\mathbb{Q}})$. Note that $E \simeq C/\Lambda$, where $\Lambda = \mathbb{Z} \oplus \mathbb{Z}\tau$ is a lattice in $\mathbb{C}$. As an abeian group the N-torsion subgroup $E[n]$ is

$$N^{-1}\Lambda/\Lambda \simeq \Lambda/N\Lambda \simeq \mathbb{Z}/N\mathbb{Z} \oplus \mathbb{Z}/N\mathbb{Z}$$

Fix a prime p. Note that multiplication by p gives a map, $\times p : E[p^{n+1}] \to E[p^n]$. Consider the system of maps,

$$\xrightarrow{\times p} E[p^{n+1}] \xrightarrow{\times p} E[p^n] \xrightarrow{\times p} \dots \xrightarrow{\times p} E[p^2] \xrightarrow{\times p} E[p]$$

The p-adic Tate-module $T_p(E)$ is the inverse limit,

$$T_p(E) = \lim_{\longleftarrow} E[p^n]$$

We have that $T_p(E) \simeq \mathbb{Z}_p \otimes \mathbb{Z}_p$. Furthermore, $T_p(E)$ is equipped with an action of $\text{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})$, which gives rise to a Galois representation,

$$\rho = \rho_{E,p} : \text{Gal}(\overline{\mathbb{Q}}/\mathbb{Q}) \to GL_2(\mathbb{Z}_p)$$

Let $\overline{\rho} : \text{Gal}(\overline{\mathbb{Q}}/\mathbb{Q}) \to GL_2(\mathbb{Z}/p\mathbb{Z})$ be the mod-p reduction of ρ. Given a prime ℓ, we set $G_\ell = \text{Gal}(\overline{\mathbb{Q}}_\ell/\mathbb{Q}_\ell)$. The inclusion $\overline{\mathbb{Q}} \hookrightarrow \overline{\mathbb{Q}}_\ell$ gives rise to an injective homomorphism $G_\ell \hookrightarrow \text{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})$. We let $\rho_{|\ell}$ be the restriction of ρ to G_ℓ. Note that $\text{Gal}(\overline{\mathbb{F}}_\ell/\mathbb{F}_\ell) \simeq \widehat{\mathbb{Z}}$, where $\widehat{\mathbb{Z}} = \lim_{\longleftarrow} \mathbb{Z}/m\mathbb{Z}$, generated by the Forbenius $\overline{\sigma}_\ell : x \mapsto x^\ell$. We shall fix a lift $\sigma_\ell \in G_\ell$ of $\overline{\sigma}_\ell$. The kernel of the reduction map $G_\ell \to \text{Gal}(\overline{\mathbb{F}}_\ell/\mathbb{F}_\ell)$ is the inertia subgroup and is denoted I_ℓ. We say that ρ is unramified at ℓ if $\rho_{|I_\ell}$ is the trivial representation. If this is the case, then $\rho(\sigma_\ell)$ is independent of the choice of lift σ_ℓ. Given an elliptic curve $E/\mathbb{Q}$, we let $a_\ell(E) = \ell + 1 - \#E(\mathbb{F}_\ell)$. The Galois representation $\rho = \rho_{E,p}$ is unramified at all primes $\ell \nmid N_p$. At a prime $\ell \nmid N_p$, the characteristic polynomial of $\rho(\sigma_e ll)$ is $\det(x \cdot \text{Id} - \rho(\sigma_\ell)) = x^2 - a_\ell(E)x + \ell$

Modular Forms and Hecke Operators

Let $\mathfrak{h}$ be the upper half plane consisting of all $z \in \mathbb{C}$ with $\Im(z) > 0$. The group $SL_2(\mathbb{Z})$ acts on $\mathfrak{h}$ by fractional linear transformations,

$$\begin{pmatrix} a & b \\ c & d \end{pmatrix} z = \frac{az+b}{cz+d}$$

Given an integer $N \geq 1$, we consider the congruence subgroups,

$$\Gamma_0(N) = \left\{ \begin{pmatrix} a & b \\ c & d \end{pmatrix} \mid c \equiv 0 \pmod{N} \right\}$$
$$\Gamma_1(N) = \left\{ \begin{pmatrix} a & b \\ c & d \end{pmatrix} \mid a, d \equiv 1 \pmod{N},\ c \equiv 0 \pmod{N} \right\}$$

We will now discuss some algebraic operators. Given $k \geq 2$, let $S_k(\Gamma_1(N), \mathbb{C})$ be the space of cuspforms of weight k on $\Gamma_1(N)$. There are 3 types of operators acting on $S_k(\Gamma_1(N), \mathbb{C})$:

- T_ℓ for every prime $\ell \nmid N$
- U_ℓ for $\ell \mid N$
- The diamond operators $\langle d \rangle$.

Let $f(z) = \sum_{n \geq 1} a_n e^{2\pi i n z}$ be the normalized Hecke eigencuspform. The fourier coefficients a_n are all algebraic numbers and generate a field extension F of $\mathbb{Q}$ such that $[F : \mathbb{Q}] < \infty$, ie., finite. We will now see what modularity of elliptic curves is. Let p be a prime and choose a prime $\mathfrak{p} \mid p$ in $\mathcal{O}_F$. Set $\mathcal{O}$ to be the completion $\mathcal{O}_F$ at $\mathfrak{p}$. Deligne showed that there is a continuous Galois representation, $\rho_{f,\mathfrak{p}} : \mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q}) \to GL_2(\mathcal{O})$, associated to f and $\mathfrak{p}$. The Galois representation $\rho_{f,\mathfrak{p}}$, is unramified at all primes $\ell \nmid N_p$, and at any prime $\ell \nmid N_p$, $\det(x \cdot \mathrm{Id} - \rho_{f,\mathfrak{p}}(\sigma_\ell)) = x^2 - a_\ell x + \ell^{k-1}\psi(\ell)$. Given $E/\mathbb{Q}$, we say that E is modular if there is a Hecke eigencuspform $f(z)$ of weight 2 on $\Gamma_0(N)$, with rational Fourier coefficients such that $\rho_{E,p} \simeq \rho_{f,p}$. If the isomorphism $\rho_{E,p} \simeq \rho_{f,p}$ holds for any one primes p, then it holds for all primes.

Theorem (Wiles, Taylor-Wiles). Every semistable elliptic curve $E/\mathbb{Q}$ is modular.

Theorem (Breuil-Conrad-Diamond-Taylor). Every elliptic curve $E/\mathbb{Q}$ is modular.

Jacobians of Modular Curves

Let $J_1(N)$ be the Jacobian of the modular curve $X_1(N)$. It is an abelian variety over $\mathbb{Q}$. We set $T_p(J_1(N))$ to be the p-adic Tate-module associated to $J_1(N)$, $T_p(J_1(N)) = \lim_{\longleftarrow} J_1(N)[p^n]$. Note that $T_p(J_1(N)) \simeq \mathbb{Z}_p^{2n}$ where $n = \dim J_1(N)$. This gives rise to a representation,

$$\rho : \mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q}) \to GL_{2n}(\mathbb{Z}_p)$$

which in fact factors through $GSp_{2n}(\mathbb{Z}_p)$.

Choose a noncanonical isomorphism of fields $\mathbb{C} \simeq \overline{\mathbb{Q}}_p$, thus view $\mathbb{Q}_p$ as a sub-algebra of $\mathbb{C}$. This isomorphism does not respect the topological structures of $\mathbb{C}$ and $\overline{\mathbb{Q}}_p$ and is highly discontinuous. Let $\mathbb{T}_N$ be the $\mathbb{Z}_p$-algebra generated by the endomorphisms of $S_2(\Gamma_1(N))$ which is generated by the Hecke operators:

- T_ℓ for $\ell \nmid N$
- U_ℓ for $\ell \mid N$

- $\langle d \rangle$, the diamond operators.

Each Hecke-operator $T \in \mathbb{T}_N$ gives rise to an endomorphism of the Jacobian $J_1(N)$, and hence an endomorphism of the Tate-module $T_p(J_1(N))$. As a result, $T_p(J_1(N))$ is viewed as a module over $\mathbb{T}_N$. A Hecke eigenform f of weight 2 gives rise to a homomorphism $\phi_f : \mathbb{T}_N \to \mathcal{O}$. Here, $T \in \mathbb{T}_N$ is sent to $\phi_f(T)$, subject to the relation, $T(f) = \phi_f(T)f$. We let $\mathfrak{m}$ be the maximal ideal generated by the kernel of ϕ_f and the uniformizer ϖ of $\mathcal{O}$. We have an isomorphism, $T_p(J_1(N))_{\mathfrak{m}} \otimes_{\mathbb{T}_{\mathfrak{m}}} \mathcal{O} \simeq \mathcal{O} \oplus \mathcal{O}$. This gives rise to the Galois representation, $\rho_{f,\mathfrak{p}} : \mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q}) \to GL_2(\mathcal{O})$.

Deformations

Let K be a finite extension of $\mathbb{Q}_p$, $\mathcal{O}$ its valuation ring and $\mathbb{F} = \mathcal{O}/\varpi$ its residue field. Let $\rho : \mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q}) \to GL_2(\mathcal{O})$ be a continuous Galois representation and $\overline{\rho} : \mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q}) \to GL_2(\mathbb{F})$ its residual representation, obtained after going modulo-ϖ. The representation ϖ lies in a family of Galois representations that are deformations of $\overline{\rho}$. A coefficient ring is a complete local noetherian $\mathcal{O}$-algbera R such that $R/\mathfrak{m}_R \simeq \mathbb{F}$. Such a ring has a presentation,

$$R \simeq \frac{\mathcal{O}[[X_1, \dots, X_m]]}{(g_1, \dots, g_k)}$$

A R-lift of $\overline{\rho}$ is a Galois representation, $\rho_R : \mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q}) \to GL_2(R)$ such that after composing with,

$$GL_2(R) \xrightarrow{\text{mod } \mathfrak{m}_R} GL_2(\mathbb{F})$$

we recover $\overline{\rho} : \mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q}) \to GL_2(\mathbb{F})$. Two lifts $\rho_1, \rho_2 : \mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q}) \to GL_2(\mathbb{F})$ are strictly equivalent if $\rho_1 = A\rho_2 A^{-1}$, for some matrix $A \in \ker(GL_2(R) \to GL_2(\mathbb{F}))$. A deformation is a strict equivalence class of lifts. Fix a finite set of primes S such that $\overline{\rho}$ is unramified at all primes $\ell \notin S$. Let G_S be the maximal quotient of $\mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})$ which is unramified at all primes $\ell \notin S$.

The Universal Deformation

Given such a choice S, there is a universal deformation of $\overline{\rho}$ which is unramified outside S. In other words, there is a deformation, $\rho^{\text{unv}} : G_S \to GL_2(R(\overline{\rho}))$ such that given any deformation $\rho_R : G_S \to GL_2(R)$, there exists unique map. $\phi : R(\overline{\rho}) \to R$ such that we recover ρ_R as the composite,

$$G_S \xrightarrow{\rho^{\text{unv}}} GL_2(R(\overline{\rho})) \xrightarrow{\phi^*} GL_2(R)$$

Local deformation conditions

We may also consider deformations of the Local Galois representation $\overline{\rho}_{|\ell} : G_\ell \to GL_2(\mathbb{F})$. Let $CLN_{\mathcal{O}}$ be the category of coefficient rings over $\mathcal{O}$. In other words, it is the category of complete, local, noetherian $\mathcal{O}$-algebras R such that $R/\mathfrak{m}_R \simeq \mathbb{F}$. Consider the functor of deformations, $\mathrm{Def}_\ell : CLN_{\mathcal{O}} \to \mathrm{Sets}$, where $\mathrm{Def}_\ell(R)$ consists of all deformations of $\overline{\rho}_{|\ell}$ to R. A deformation condition $\mathcal{C}_\ell$ is an subfunctor of Def_ℓ, satisfying further conditions that make it representable. As a functor, it takes every coefficient ring R to a set of local deformations $\mathcal{C}_\ell(R) \subseteq \mathrm{Def}_\ell(R)$ in a functorial way. We say that a deformation $\varrho : G_\ell \to GL_2(R)$ satisfies the deformation condition $\mathcal{C}_\ell$ if $\varrho_R \in \mathcal{C}_\ell(R)$. A deformation type $\mathcal{D} = (\Sigma, \{\mathcal{C}_\ell\}_{\ell \in \Sigma})$ for $\overline{\rho}$ consists of the following data:

1. A set of primes Σ outside of which $\overline{\rho}$ is unramified.

2. At each prime $\ell \in \Sigma$, a deformation condition $\mathcal{C}_\ell$.

The Taylor-Wiles method

Let $E/\mathbb{Q}$ be an elliptic curve and consider the prime $p = 3$. Then, there are 2 cases to consider:

1. $\overline{\rho} = \overline{\rho}_{E,3}$ is absolutely irreducible. In this case, it is known that $\overline{\rho}$ is modular by the result of Langlands and Tunnell.

2. $\overline{\rho}$ is not absolutely irreducible. In this case the prime 3 may be replaced by the prime 5 and the representation $\overline{\rho}_{E,5}$ is absolutely irreducible.

Let N_0 be the prime to p part of the Artin-conductor of $\overline{\rho}$. Let $\mathbb{T}_0$ be the Hecke algbera at minimal level N_0 localized at an appropriate maximal ideal (associated to $\overline{\rho}$). On the other hand, there is a minimal deformation type $\mathcal{D}_{\min} = (S, \{\mathcal{C}_\ell\}_{\ell \in S})$. Here, $S = \{\text{primes } q : q \mid N_0 p\}$. Let R_0 be the universal deformation ring $R_{\mathcal{D}_{\min}}$. Note that from the Jacobian, we have a Galois representation associated with $\mathbb{T}_0$, $\rho' : \mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q}) \to GL_2(\mathbb{T}_0)$. The representation ρ' satisfies all deformation conditions $\mathcal{C}_\ell$ prescribed by the type $\mathcal{D}_{\min}$. By the universal property, we obtain a map $\varphi_0 : R_0 \to \mathbb{T}_0$. The goal is to prove that φ_0 is an isomorphism. Such a result needs to be proven at non-minimal levels as well, but this requires a slightly more involved argument. An result establishing an isomorphism between a deformation ring R and a localized Hecke algebra $\mathbb{T}$ is known as an "$R = \mathbb{T}$" theorem. The representation ρ associated with an elliptic curve coincides with a map $R \to \mathbb{Z}_p$. Since $R \simeq \mathbb{T}$, it follows that this map is the same as a map $\mathbb{T} \to \mathbb{Z}_p$. Finally, it is not hard to prove that any homomorphism $\mathbb{T} \to \mathbb{Z}_p$ is one associated to a Hecke eigenform f, taking a Hecke operator T to the eigenvalue $\phi_f(T)$.

Taylor-Wiles primes

A prime number q is a Taylor-Wiles primes if $q \notin S$, $q \equiv 1 \pmod p$ and $\overline{\rho}(\sigma_q)$ is semisimple with distinct eigenvalues. Let $Q = \{q_1, \ldots, q_r\}$ be a finite set of Taylor-Wiles primes. Define a new deformation condition $\mathcal{D}_Q = (S \cup Q, \{\mathcal{C}_\ell\}_{\ell \in S \cup Q})$ by allowing ramification at the primes $q \in Q$. Let R_Q be the associated deformation ring. We will now compare deformation rings. The universal deformation of type-$\mathcal{D}_0$ is also of type $\mathcal{D}_Q$. Hence, there is a natural homomorphism, $R_Q \to R_0$. Let Δ_q be the p-primary part of $(\mathbb{Z}/q\mathbb{Z})^\times$. Set Δ_Q to be the product,

$$\Delta_Q = \prod_{q \in Q} \Delta_q$$

The deformation ring R_Q associated to $\mathcal{D}_Q$ is an $\mathcal{O}[\Delta_Q]$-algebra. Letting $\mathfrak{a}_Q$ be the augementation ideal in $\mathcal{O}[\Delta_Q]$, there is an isomorphism, $R_Q/\mathfrak{a}_Q R_Q \simeq R_0$. Likewise, there is a localized Hecke algbera associated wuth the type $\mathcal{D}_Q$, which we denote by $\mathbb{R}_Q$. As in the case with deformation rings, $\mathbb{T}_Q$ is an $\mathcal{O}[\Delta_Q]$-algebra and there is an isomorphism, $\mathbb{T}_Q/\mathfrak{a}_Q\mathbb{T}_Q \simeq \mathbb{T}_0$. There is a natural map $\varphi_Q : R_Q \to \mathbb{T}_Q$, such that the following square commutes,

$$\begin{array}{ccc} R_Q & \xrightarrow{\varphi_Q} & \mathbb{T}_Q \\ \downarrow & & \downarrow \\ R_0 & \xrightarrow[\varphi_0]{} & \mathbb{T}_0 \end{array}$$

Patching

There exists $r \geq 1$ such that for every $n \geq 1$, there is a set Q_n of r Taylor-Wiles primes such that $q \equiv 1 \pmod{P^n}$. Set $R_n = R_{Q_n}$ and $\mathbb{T}_n = \mathbb{T}_{Q_n}$. Given Q_n, the set of primes Q_{n+1} can be constructed in a way so that there are natural maps $R_{n+1} \to R_n$ and $\mathbb{T}_{n+1} \to \mathbb{T}_n$ so that the following diagram commutes,

$$\begin{array}{ccc} R_{n+1} & \longrightarrow & \mathbb{T}_{n+1} \\ \downarrow & & \downarrow \\ R_n & \longrightarrow & \mathbb{T}_n \end{array}$$

A set $\Delta_n = \Delta_{Q_n}$. Note that R_n and $\mathbb{T}_n$ are algberas over,

$$\mathcal{O}[\Delta_n] \simeq \frac{\mathcal{O}[S_1, \dots, S_r]}{((1+S_1)^{p^n} - 1, \dots, (1+S_r)^{p^n} - 1)}$$

Taking the inverse limit $\mathcal{O}_\infty = \lim_{\longleftarrow} \mathcal{O}[\Delta_n]$ is a formal power series ring over $\mathcal{O}$ in r-variables,

$$\mathcal{O}_\infty \simeq \mathcal{O}[[S_1, \dots, S_r]]$$

Set $R_\infty = \lim_{\longleftarrow} R_n$ and $\mathbb{R}_\infty = \lim_{\longleftarrow} \mathbb{T}_n$. Let $\varphi_\infty : R_\infty \to \mathbb{T}_\infty$ be the inverse limit of the maps $\varphi_n : R_n \to \mathbb{T}_n$. Note that $R_0 = R_\infty/(S_1, \dots, S_r)$ and $\mathbb{T}_0 = \mathbb{T}_\infty/(S_1, \dots, S_r)$. If it is shown that $\varphi_\infty : R_\infty \to \mathbb{T}_\infty$ is an isomorphism, then it shall follow that $\varphi_0 : R_0 \to \mathbb{T}_0$ is an isomorphism as well. Each Hecke-algebra $\mathbb{T}_n$ acts faithfully on a space of modular forms M_n which is finitely generated and free as an $\mathcal{O}[\Delta_n]$-module. Letting $M_\infty = \lim_{\longleftarrow} M_n$, we find that M_∞ is a finitely generated free $\mathcal{O}_\infty = \mathcal{O}[[S_1, \dots, S_r]]$-module. It follows from this that $\mathbb{T}_\infty$ is also a finitely generated and faithful $\mathcal{O}_\infty$-module. On the other hand, it follows from Galois theoretic arguments that R_∞ is a quotient of $\mathcal{O}[[X_1, \dots, X_r]]$. By the dimension considerations, $R_\infty = \mathcal{O}[[X_1, \dots, X_r]]$. Since $R_\infty \to \mathbb{T}_\infty$ is a surjective and $\mathbb{T}_\infty$ is faithful over $\mathcal{O}[[S_1, \dots, S_r]]$, this implies that φ_∞ must be an isomorphism.