Seminar on Potential Modularity and its Applications

Panagiotis Tsaknias

April 1, 2011

1 Intro

A main theme of modern (algebraic) number theory is the study of the absolute Galois group $G_\mathbb{Q}$ of $\mathbb{Q}$ and more specifically its representations. Although one dimensional Galois representations admit an elegant description through class field theory, the general case is nowhere near that easy to handle. The well known Langlands Program is a far reaching web of conjectures that was devised in effort to describe such representations.

On one side one has analytic objects (automorphic representations) whose behavior is “better understood”, i.e. the $L$-function associated with them admits an analytic continuation to the whole complex plane and satisfies a functional equation. On the other side, one has $L$-series that come from Galois representations and whose analytic continuation and functional equation is difficult to show. The Langlands program suggests that one can indirectly prove that by showing that the Galois representation in question is associated with an automorphic representation, i.e. they are associated with the same $L$-function.

One of the first examples of this approach was the classical proof that CM elliptic curves are modular, and therefore their $L$-function admits an analytic continuation and satisfies a functional equation.

For more general classes of elliptic curves the first major breakthrough was done by Wiles [22] and Taylor-Wiles [19] who proved that all semisimple elliptic curves are modular. Subsequent efforts culminating with the work done by Breuil-Conrad-Diamond-Taylor [2] finally proved modularity for all elliptic curves over $\mathbb{Q}$.

To an elliptic curve $E$ one can attach a Galois representation $\rho_{E,p}: G_\mathbb{Q} \rightarrow \text{GL}_2(\mathbb{Q}_p)$ for every prime $p$. $E$ being modular is equivalent to all the $\rho_{E,p}$ (or again equivalently just one of them) being modular. With this in mind, Wiles method and its refinements boil down to the following steps:

1. Pick (actually show that you can find) a representation $\rho_{E,p}$ out of the ones attached to $E$ for each prime, such that $\bar{\rho}_{E,p}$, i.e. its reduction mod $p$, is modular.

2. Use (actually prove) a theorem of the form: "If $\bar{\rho}$ is irreducible and modular + other conditions $\Rightarrow \rho$ is modular". I will use the abbreviation $MLT$ to refer to theorems of this kind from now on.

Wiles fully exploited the fortunate coincidence that the representation $\rho_{E,3}$, when reduced mod 3 gives a representation whose image lies in $\text{GL}_2(\mathbb{F}_3)$. The latter is a solvable group and work from Langlands [11] and Tunnell [20] in the late 70’s-early 80’s showed that representations with solvable image are modular. If we assume that $\bar{\rho}_3$ is irreducible then
all one needs is to prove an MLT. Wiles had the insight\(^1\) that if \(\rho_3\) is not irreducible then there exists another elliptic curve \(E'\) such that:

- \(E[5] \cong E'[5]\) is irreducible
- \(E'[3]\) is irreducible.

One can now use the MLT to show that \(E'\) is modular because \(E'[3]\) is, and therefore \(E[5] \cong E'[5]\) is and apply the MLT to \(\rho_{E,5}\) to get that \(E\) is modular as required.

Unfortunately the case of elliptic curves over \(\mathbb{Q}\) is rather an exception and one should not expect to be lucky enough to have an obvious residual representation that is (easily seen to be) modular.

### 2 Potential modularity

As we saw an obvious limitation of the MLTs proved by Wiles and his successors was that they require something modular as input. They “transfer” modularity instead of “creating” it. In his two papers [17] and [18], Taylor introduces a really clever idea that almost circumvents this problem: Instead of trying to prove that a given \(p\)-adic representation \(\rho\) of \(G_{\mathbb{Q}}\) (that of course satisfies some conditions) is modular, he allowed himself to consider restrictions of his representation to \(G_F\) for arbitrary totally real fields \(F\) and try to prove that one of these is modular. Indeed he managed to show that one (under suitable assumptions) can always find such an extension \(F/\mathbb{Q}\), an abelian variety \(A\) over \(F\) and a totally real field \(M\) such that:

- \(\mathcal{O}_M \hookrightarrow \text{End}(A)\),
- \(A[p] \cong \bar{\rho}|_{G_F}\), where \(\bar{\rho}\) is the reduction mod \(p\) of \(\rho\),
- \(A[l] \cong \text{Ind} \theta\) for some character \(\theta\) of a quadratic extension of \(F\).

Here \(p\) and \(l\) are two primes of \(M\) above the distinct rational primes \(p\) and \(\ell\) respectively. One can clearly see the similarities with Wile’s prime-switch trick here: Taylor provides a compatible system of representations (the one associated with \(A\)) that is modular (because one of the reductions, the one at \(l\), is an “easy” case) and agrees residually (at the other prime \(p\)) with \(\rho|_{G_F}\) (and thus transferring modularity to \(\rho|_{G_F}\)). Of course here one needs to provide an MLT for totally real fields in order transfer modularity from \(A[l]\) to \(A\) and from \(\bar{\rho}|_{G_F} \cong A[p]\) to \(\rho|_{G_F}\). In Taylor’s case these were provided by work of Diamond [4], Fujiwara [6], Skinner and Wiles [14], [15] and by his work [18]. Finally one can perhaps now see why such a representations is called “potentially modular”. Our initial representation is only proven to be modular after restriction to another absolute Galois group. One important thing however about this result is that, unlike its predecessors, it doesn’t require a modularity assumption to provide modularity.

The goal of this seminar is to explain the details involved in Taylor’s adaption of Wiles’ trick and explain what applications such a result has. Let us just mention that by using Brauer’s induction theorem one can show the meromorphic continuation of the \(L\)-series associated to \(\rho\) and get a functional equation. Finally more recent work on potential

---

\(^1\)There is also the case that \(E[5]\) is also reducible but all such elliptic curves have been checked to be modular
modularity of $n$ dimensional representations (which uses the same basic idea of Wiles’ prime-switch trick) was used to prove the Sato-Tate conjecture.

As a final remark let us mention that although such a result may nowadays seem unnecessary due to the proof of Serre’s conjecture, Taylor’s potential modularity result is a crucial initial ingredient in its proof.

3 Schedule of the talks

1st talk, April 7th, Survey of Potential Modularity and the Seminar, Gabor Wiese

State the main theorems concerning potential modularity of a Galois representation $\rho$ and explain briefly the notions involved.

Distribution of the remaining talks.

2nd talk, April 14th, Hilbert Modular Forms (HMF), Nicolas Billerey

Definitions and facts about Hilbert modular forms (HMF) and automorphic representations for $GL_{2,F}$ (following [21]). Hecke theory, eigenforms. Hecke maps $\mathbb{T} \to \mathbb{C}$. The adelic picture should be mentioned. Sections 13–15 of [9] might prove useful as well.

3rd talk, April 28th, Galois Representation attached to a HMF, Panagiotis Tsaknias

Sketch of construction over $\mathbb{Q}$ following Section 16.2 of [9]. Compatible systems of Galois representations. Modularity of induced Galois representations: Theorems (3.3.1) and (4.3.15) leading to (4.8.2), all from [12]. Statement of the Langlands-Tunnell theorem if time allows.

4th talk, May 5th, and 5th talk, May 12th, Skolem Problems

Let $K$ be a number field and $S$ a finite set of absolute values on $K$. We define $K_S$ to be the maximal extension of $K$ such that every $v \in S$ totally splits in $K_S$. The aim of these two talks is to prove a theorem of Moret-Bailly and Pop that asserts that $K_S$ satisfies a Rumely type local-global principle: If $V$ is a geometrically irreducible $K_S$-variety that has a smooth point in every completion at $v \in S$, then $V$ has a $K_S$ rational point.

Plan of talks:

- Formulation of the theorem and some examples
- Presenting without a proof the necessary topological theorems
  - The continuity of roots of algebraic functions
  - The $\nu$-adic implicit function theorem
  - The open image theorem
- Proof of the main theorem
• Proof of some generalizations of the main theorem that are needed to potential modularity

To understand the proof one needs to possess some knowledge in algebraic geometry. A quick proof of the theorem can be found in Gunther Cornelissen’s notes [3]. A detailed proof that includes also proofs of the topological statements and treat the positive characteristic case can be found in [8]. Finally deduce the generalizations [16], Propositions 5.2.2 and 8.2.2.

The subdivision of the two talks will be decided by the speakers.

6th talk, May 19th, Modularity Lifting Theorems (MLT)

This talk surveys modularity lifting theorems, following for example [16], Sections 3 and 4, Section 3 of [23], or [1]. For the seminar we need the MLT stated in [16], Theorem 4.4.2.

The talk requires some previous familiarity with these objects.

7th talk, May 25th, and 8th talk, June 9th, Hilbert-Blumenthal Abelian Varities (HBAV) - Moduli Space

These two talks are concerned with the definitions, notions and theorems appearing in the proof of [16], Proposition 5.3.1. This proposition will be explained and proved in the 9th talk; here, the aim is to provide all ingredients. In particular, the definitions and notation concerning Hilbert-Blumenthal abelian varieties need be introduced. The existence and geometric properties of the corresponding moduli scheme $X$ should be explained as well. For the proof that $X$ is geometrically connected follow [13]. Show the existence statements of points over $\overline{F}_v$ for $v \in \Sigma$. It might be useful to consult Section 1 of [17].

Another useful reference might be Chapter 3 and Chapter 6 of [7].

Some previous familiarity with these objects will be very helpful. The speakers subdivide the talks themselves.

9th talk, June 16th, Proof of Potential Modularity

State and prove [16], Proposition 5.3.1, which provides a unifying framework for everything mentioned in the previous talks. Prove Proposition 5.4.1 regarding the existence of ‘easily seen to be modular’ Galois representations. Finally proceed to the proof of Theorem 5.1.1 and then to that of 5.1.2 as in [16]. The proof of Lemma 4.2.2 is also needed there.

10th talk, June 30th, Meromorphic continuation of L-functions, Sara Arias-de-Reyna

In the subsequent talks, important corollaries of potential modularity will be treated. In this talk, we focus on the meromorphic continuation certain L-functions. Follow Sections 9.1, 9.2 and 9.3 of [16].
11th talk, July 7th, Cases of the Fontaine-Mazur Conjecture

Follow Section 9.4 of [16]. You will need Theorem 7.6.1 of [16] (which you will state without proof) and Proposition 8.2.1 which can be derived by Propositions 8.1.1 and 8.2.2 (already proven in talk 5, just recall it).

12th talk, July 14th, Serre’s modularity conjecture

Overview of the proof of Serre’s modularity conjecture (see [10] or [5]).

References


