Number Theory Seminar
Spring, 2018: Modularity

Motivation

The main topic of the seminar is the "classical" theory of modularity à la Wiles, Taylor–Wiles, Diamond, Conrad, Breuil, Kisin,.... Modularity grew out of the proof of Fermat's Last Theorem as orchestrated by A. Wiles. As is well known, and not especially relevant to the topic this semester, the construction of G. Frey begins with a purported counterexample to Fermat's Last Theorem for exponent p ($p > 5$, say) and produces a semistable elliptic curve that was shown (by me) not to be modular. To derive a contradiction, Wiles and Taylor–Wiles showed that the curve is *modular*.

In the most straightforward situation, the mod 3 Galois representation

$$\rho : \mathrm{Gal}(\overline{\mathbf{Q}}/\mathbf{Q}) \to \mathbf{GL}(2, \mathbf{F}_3)$$

arising from the elliptic curve is irreducible (and therefore surjective). The 3-adic Galois representation attached to the curve is a lift (= deformation)

$$\tilde{\rho} : \mathrm{Gal}(\overline{\mathbf{Q}}/\mathbf{Q}) \to \mathbf{GL}(2, \mathbf{Z}_3)$$

of ρ. If $\tilde{\rho}$ can be shown to be modular (in the sense that it arises from a weight 2 cusp form on $\Gamma_0(N)$, where N is the conductor of the curve), then the curve is modular and we get a contradiction. A major theorem of Langlands from the 70s ("Base change for GL(2)") yields the modularity of ρ. (This semester, we take the work of Langlands as given.) Once Langlands's theorem is admitted, the modularity of $\tilde{\rho}$ can be deduced from a *modularity lifting theorem*

$$\rho \text{ modular} \stackrel{?}{\Longrightarrow} \tilde{\rho} \text{ modular}.$$

Proving a modularity lifting theorem is the goal of this semester's series of lectures.

A precise-sounding result

The minimal sort of result that we could prove would go as follows. Let p be an odd prime and let $\tilde{\rho}$: $\mathrm{Gal}(\overline{\mathbf{Q}}/\mathbf{Q}) \to \mathbf{GL}(2, \mathbf{Z}_p)$ be a continuous Galois

representation that has the "same" local behavior (at each prime including p) that we'd see in the p-adic representation attached to a weight 2 cuspidal newform on $\Gamma_0(N)$ where N is a *square free* integer. Let ρ: $\mathrm{Gal}(\overline{\mathbf{Q}}/\mathbf{Q}) \to \mathbf{GL}(2, \mathbf{F}_p)$ be the mod p reduction of $\tilde{\rho}$. Assume:

- that ρ is irreducible;
- that ρ has the same qualitative local behavior as $\tilde{\rho}$. The second condition is intended to convey the idea that ρ does not accidentally happen to be less ramified than its lift $\tilde{\rho}$. For example, if N is prime to p, one requires that the "Serre conductor" of ρ (which is just the prime-to-p part of the Artin conductor of ρ) be equal to N (and not some proper divisor of N).

Under these conditions, one proves:

THEOREM *The representation $\tilde{\rho}$ is* modular *in the sense that it arises from a weight 2 newform on $\Gamma_0(N)$.*

One can go beyond this theorem in various directions:

- We can suppress the second condition, allowing ρ to be accidentally less ramified than $\tilde{\rho}$. This is necessary for the application to Fermat's Last Theorem because the mod p Galois representation attached to a semistable elliptic curve can easily have a smaller conductor than one might expect: the minimal discriminant of the curve could have an exponent at some prime ℓ that is divisible by p (p divides n, where $\ell^n || \Delta_E$). In Chapter 3 of his "Fermat" article, Wiles explains how to interpolate between the "minimal" case where the second condition is satisfied and the general case where the second condition might not be satisfied.
- We can remove conditions of semistability. This is the work that was done by Conrad, Diamond, Breuil, Taylor in the late 1990s.
- We can try to generalize everything as much as possible, moving from $\mathbf{GL}(2,)$ to other reductive groups. For this, one needs to read Kisin, Taylor,.... I am even less of an expert here than in the simple case that is our main topic this semester.

The idea of the proof is to prove an isomorphism of rings "$\mathcal{R} = \mathbf{T}$," where $\mathcal{R}$ is a "deformation ring" that classifies all deformations of ρ with appropriate local behavior and $\mathbf{T}$ is a p-adic Hecke algebra that controls modular deformations. After constructing $\mathbf{T}$, one finds a deformation

$$\mathrm{Gal}(\overline{\mathbf{Q}}/\mathbf{Q}) \to \mathbf{GL}(2, \mathbf{T})$$

of ρ; i.e., one pieces together a Galois representation associated to $\mathbf{T}$. This deformation induces a ring homomorphism

$$\mathcal{R} \to \mathbf{T};$$

one then "only" needs to establish that this homomorphism is an isomorphism.

The original proof that "$\mathcal{R} = \mathbf{T}$" was given by Taylor–Wiles in their short paper that "completed" Wiles's proof of Fermat's Last Theorem. (My theorem was analogously a prequel.) A different perspective on the Taylor–Wiles proof was supplied by G. Faltings before the proof was published; Faltings's version appears as an appendix to Taylor–Wiles. A simplification was supplied very soon afterwards by F. Diamond; this is in a separate article.

Calendar

January 24 This organizational meeting.

January 31 Intro to theory of Galois representations, following Mazur [5].

February 7 A second lecture on Mazur's article [5].

February 14 This may be overkill, but a third lecture on [5].

February 21 A description of the Hecke algebra $\mathbf{T}$ and the p-adic representation $\rho_{\mathbf{T}}\colon \mathrm{Gal}(\overline{\mathbf{Q}}/\mathbf{Q}) \to \mathbf{GL}(2, \mathbf{T})$. A reasonable reference for this is the discussion in §3 of [4]; also, see [6], §24.

February 28 Back to deformations, starting with §2.7 of [1]. A discussion of §2.8 of [1], "Special cases."

March 7 AWS: some people will be away. Perhaps we can have a one-off talk on a topic not related to modularity.

March 14 A proof of the $\mathcal{R} = \mathbf{T}$ theorem in the minimal case, following §3.5 of [1], or the article [2].

March 21 Continuation of: A proof of the $\mathcal{R} = \mathbf{T}$ theorem in the minimal case, following §3.5 of [1], or the article [2].

March 28 Spring recess—no seminar meeting.

April 4 Moving from the minimal case to the general case.

April 11 Discussion of "multiplicity one" results: the fact that Tate modules tend to be locally free of rank 1 over Hecke rings. These results were used in Wiles's original proof but were circumvented by [3].

April 18 An exposition of Fred Diamond's article [3]. What is Diamond's new idea?

April 25 Catching up and completing arguments. We probably didn't allow enough time for all the main points to be exposed. Alternative idea: How did Kisin go beyond Taylor–Wiles systems?

May 2 RRR week

May 9 Exam week

May 16 Graduation week

References

[1] Henri Darmon, Fred Diamond, and Richard Taylor. Fermat's last theorem. In *Elliptic curves, modular forms & Fermat's last theorem (Hong Kong, 1993)*, pages 2–140. Int. Press, Cambridge, MA, 1997.

[2] Ehud de Shalit. Hecke rings and universal deformation rings. In *Modular forms and Fermat's last theorem (Boston, MA, 1995)*, pages 421–445. Springer, New York, 1997.

[3] Fred Diamond. The Taylor-Wiles construction and multiplicity one. *Invent. Math.*, 128(2):379–391, 1997.

[4] Fred Diamond and Kenneth A. Ribet. l-adic modular deformations and Wiles's "main conjecture". In *Modular forms and Fermat's last theorem (Boston, MA, 1995)*, pages 357–371. Springer, New York, 1997.

[5] Barry Mazur. An introduction to the deformation theory of Galois representations. In *Modular forms and Fermat's last theorem (Boston, MA, 1995)*, pages 243–311. Springer, New York, 1997.

[6] Keneth A. Ribet and William Stein. Lectures on modular forms and hecke operators. https://wstein.org/books/ribet-stein/main.pdf.

[7] Richard Taylor and Andrew Wiles. Ring-theoretic properties of certain Hecke algebras. *Ann. of Math. (2)*, 141(3):553–572, 1995.

[8] Andrew Wiles. Modular elliptic curves and Fermat's last theorem. *Ann. of Math. (2)*, 141(3):443–551, 1995.