LECTURE 25: ATKIN-LEHNER-LI THEORY, EICHLER-SHIMURA THEORY, AND MOTIVATING IDEAS BEHIND THE PROOF OF FERMAT'S LAST THEOREM

LARRY ROLEN, VANDERBILT UNIVERSITY, FALL 2020

> I think I'll stop here.
>
> Sir Andrew Wiles, After finishing writing the proof to Fermat's Last Thereom (June 23, 1993), as quoted by Simon Singh (1997). Fermat's Enigma: The Quest to Solve the World's Greatest Mathematical Problem. Viking. p. 33.

1. Newforms and Atkin-Lehner-Li Theory

We saw before that the **level of a modular form isn't unique**. Specifically, for all $d \geq 1$,

$$M_k(N) \subseteq M_k(Nd).$$

This is similar to how a Dirichlet character isn't periodic with respect to a unique modulus. We've seen examples of Dirichlet characters, but to be precise let's briefly define them. We say $\chi \colon \mathbb{Z} \to \mathbb{C}$ is a **Dirichlet character of modulus** k if its completely multiplicative ($\chi(mn) = \chi(m)\chi(n)$ for all m, n), satisfies $\chi(n+k) = \chi(n)$, and is zero at n if and only if $(n, k) > 1$. As, for instance, a 5-periodic function is also 10-periodic, the modulus isn't unique. However, there is a unique **smallest** period of repetition, called the **conductor**. A character is called **primitive** if it doesn't come trivially from a character of smaller modulus. On the level of L-functions, imprimitive characters aren't nice. Specifically, their L-functions have "missing" Euler factors.

We also want to count modular forms as "old news" if they "come" from modular forms of lower level in a simple way. Recall that the V_m-operator $f|V_m(\tau) = f(m\tau)$ multiplies the level by m. We say that $f \in M_k(mN)$ is **old** if $f = g|V_m$ for some $g \in M_k(N)$. The span of all the old forms is denoted by $M_k^{\mathrm{old}}(N)$. The space of **forms which are new** is $M_k^{\mathrm{new}}(N)$, the orthogonal complement of $M_k^{\mathrm{old}}(N)$ with respect to the Petersson inner product.

Any time you have a new structure of modular forms, you should ask how it plays with Hecke operators. The same sort of application of the Spectral Theorem as before can be used to show that $S_k(N)$ has a basis of eigenforms of the operators T_p **only** for $p \nmid N$. On $S_k^{\mathrm{new}}(N)$, there is the deep **Atkin-Lehner-Li theory:** $S_k^{\mathrm{new}}(N)$ has a unique (up to reordering) basis of normalized eigenforms for **all** T_p, even those with $p|N$.

Since

$$S_k(N) \cong \oplus_{d|N} S_k^{\text{new}}(d)|V_{\frac{N}{d}},$$

this gives a nice **canonical** basis for the full space $S_k(N)$. These forms are called the **newforms**.

Newforms aren't the same as "forms which are new."

2. Newforms and the Modularity Theorem

Recall that the **conductor of an elliptic curve** is a refinement of the discriminant which keeps track not only of the bad primes bad also exactly how they are bad. The **full statement of the Modularity Theorem** is really that to any rational elliptic curve E of **conductor** N, there is a **newform** f_E of weight 2 and level N such that

$$L(E, s) = L(f, s).$$

3. Eichler-Shimura Theory

This incredibly difficult theorem is well beyond what we can accomplish this semester. However, there is a converse which was well-known prior to its proof, **Eichler-Shimura theory**. I will give a sketch of how this works without proof. Given a modular form $f = \sum_n a_n q^n$ in this space, recall that D intertwines slashing in weights 0 and 2. Hence the antiderivative, which we call an **Eichler integral**, $F := \sum_n \frac{a_n}{n} q^n$ satisfies:

$$D(F|_0(1-\gamma)) = (DF)|_2(1-\gamma) = f|_2(1-\gamma) = 0 \quad \forall \gamma \in \Gamma_0(N).$$

Thus, the error to modularity for any γ is a constant:

$$F|_0(1-\gamma) \in \mathbb{C}.$$

This gives a *map*:

$$\psi \colon \Gamma_0(N) \to \mathbb{C}$$

sending

$$\gamma \mapsto F|_0(1-\gamma)$$

It turns out that the image of Ψ is a **lattice**. Then $\mathbb{C}/\psi(\Gamma_0(N))$ is the corresponding elliptic curve which relates to f under the Modularity Theorem.

4. Ideas behind the proof of Fermat's Last Theorem

Why does the Modularity Theorem imply Fermat's Last Theorem (FLT)? This is not at all obvious. The connection that led to this eventual proof, first considered by Hellegouarch, is to relate a solution to what is now called a **Frey curve**. It is easy to show that to prove FLT it suffices to consider the case of prime exponents and exponent 4 (this last case is classical). Let (a, b, c) be a "forbidden" primitive solution (the numbers are coprime) to the equation

$$a^p + b^p = c^p.$$

If A, B, C are coprime with $A+B+C=0$ and $A, B, C \neq 0$, then the equation

$$E_{A,B,C}\colon y^2 = x(x-A)(x+B)$$

defines an elliptic curve with discriminant $16A^2B^2C^2$. Thus, to any triple a, b, c giving a solution to FLT, we can form the Frey curve $E_{a^p,b^p,-c^p}$.

Example. *Solutions do exist when* $p=2$*, namely, the Pythagorean triples. The simplest of these is* $(3,4,5)$*. The corresponding Frey curve is*

$$E_{9,16,-25}\colon y^2 = x(x-9)(x+16).$$

It turns out that this is the **modular curve** $X_0(15)$*, namely, the compactification obtained by adding cusps to* $\Gamma_0(15)\backslash \mathrm{SL}_2(\mathbb{Z})$*.*

The key observation of Frey was then the following: if (a, b, c) solve Fermat's equation with exponent $p > 2$, then the corresponding Frey curve has “strange properties.” One then suspects that these are too strange to hold for any elliptic curve. It turns out, as Serre and Ribet showed, that these cannot be satisfied is the elliptic curve is modular, as the additional structure of modular forms prohibits such behavior.

Further, the conductor is the **radical** of abc (the product of distinct primes dividing abc). Thus, the conductor is square-free (we say that the elliptic curve is **semistable**). Wiles thus only had to prove the modularity theorem in these squarefree cases to imply FLT. Ribet's step was to prove a level-lowering result which allows one to strip off primes from the modular forms levels to eventually get to $M_2(2)$, an empty space.

If you have heard of the **abc Conjecture**, then the above may sound familiar. A related conjecture, due to Szpiro, states the following relationship between elliptic curve discrimianants and conductors:

$$|\Delta| \ll N^{6+\varepsilon}.$$

This is sufficient to prove FLT for sufficiently large exponents, but is still open. However, if we could prove things like abc and Szpiro, we'd have an alternative way to asymptotically prove things like FLT.

Finally, it is important to mention that this is a powerful method that can be used to study other sorts of Diophantine equations, and is by no means limited to specific problems like FLT. For instance, we have the following recent Annals result which used the method of Frey curves and the Modularity Theorem:

Theorem (Bugeaud, Mignotte, Siksek (2006))**.** *The largest perfect power Fibonacci number is* 144*.*