LECTURE 26: APPLICATIONS TO THE CONGRUENT NUMBER PROBLEM

LARRY ROLEN, VANDERBILT UNIVERSITY, FALL 2020

For a fundamental discriminant $0 > D \equiv 5 \pmod 8$ with $3|D|$ not a square, consider the finite sums over quadratic forms $[a, b, c]$ of discriminant $-3D$:

$$A := \sum_{\substack{b^2-4ac=-3d \\ a+3b+9c>0>a \\ 32|a}} \chi([a,b,c]),$$

$$B := \sum_{\substack{b^2-4ac=-3d \\ c>0>a \\ 32|a}} \chi([a,b,c])$$

with $\chi([a,b,c])$ equal to $\left(\frac{-3}{a}\right)$ if $3 \nmid a$, and equal to $\left(\frac{-3}{c}\right)$ if $3|a$. Then under BSD,

$$|D| \text{ is a congruent number} \iff A = B.$$

Theorem of Ehlen-Guerzhoy-Kane-Rolen giving an alternative way to test if numbers are congruent; we'll give a different formula due to Tunnell later.

Recall from earlier that if we want to determine if n is congruent, we want to test if the rank $\operatorname{rk}(E_n)$ is positive or not. Assuming BSD,

$$n \text{ is congruent} \iff \operatorname{rk}(E_n) > 0 \iff L(E_n, 1) = 0.$$

Now each E_n is related to a weight 2 newform by the Modularity Theorem (or, as we saw, its related to a theta series for a Hecke character, without the full power of the Modularity Theorem required).

We also saw that E_n is the n-th **quadratic twist** of the congruent number curve E_1. As the elliptic curves E_n are obtained in an easy way from E_1, its natural to ask whether the same holds for their modular form counterparts. This is indeed true.

Definition. Given a cusp form $\sum a_n q^n f \in S_k^{\text{new}}(N)$, and given a d such that $(d, N) = 1$, define its **quadratic twist** by the character $\chi_d := \left(\frac{d}{\cdot}\right)$ as the q-series

$$(f \otimes \chi_d)(\tau) := \sum \chi_d(n) a_n q^n.$$

This twist is a modular form:

$$f \otimes \chi_d \in S_2(16Nd^2).$$

This plays the same role on the modular forms side as quadratic twists play on the elliptic curve side. Specifically, if n is squarefree and $L(E, s) = L(f, s)$ for a rational elliptic curve E and a corresponding weight 2 newform f, then

$$L(E(d), s) = L(f \otimes \chi_d, s),$$

where we recall that $E(d)$ denotes the d-th quadratic twist of E in general.

Thus, determining if n is congruent boils down to studying when $L(f \otimes \chi_n, 1)$ vanishes, where f is a weight 2 newform of level the conductor of E_1 (this happens to be 32). How should we expect these vanishing values to vary on average for different choices of d? It turns out we can say a lot without too much work. For this, we first require the specific shape of the functional equations for our L-functions.

Definition. Let f be an even weight $2k$, level N newform. Recall the **Fricke involution**:

$$W_N := \begin{pmatrix} 0 & -1 \\ N & 0 \end{pmatrix}.$$

Acting on the upper half plane, this is indeed an involution, and so

$$f|W_N = \pm f.$$

We call this sign $\varepsilon(f)$; that is, $f|W_n = \varepsilon(f)f$. The completed L-function is then

$$\Lambda(f,s) := \left(\frac{2\pi}{\sqrt{N}}\right)^{-s} \Gamma(s)L(f,s).$$

This satisfies the functional equation

$$\Lambda(f,s) = \varepsilon(f)(-1)^{-k}\Lambda(f, 2k-s).$$

That is, $\varepsilon(f)(-1)^k$ is the **sign of the functional equation**.

In particular, for elliptic curves, we have the same completion, and then we have a functional equation whose sign of the functional equation we denote by w_E:

$$\Lambda(E,s) = w_E\Lambda(E, 2-s).$$

We call this number w_E the **root number**.

In families of quadratic twists, the root number is easy to determine, as:

$$w_{E(d)} = w_E\chi_d(-N).$$

The point is that this root number determines the **parity of the order of vanishing** of $L(E,1)$. Elliptic curves with larger rank are rare, and one expects that "most of the time," an elliptic curve takes the minimal rank which this restriction allows. That is, if $w_E = +1$, then under BSD, the rank is an even number, and most likely 0. If, on the other hand $w_E = -1$, then the rank is an odd number, **automatically non-zero**.

Thus, under BSD, in families of quadratic twists, we can easily produce many examples of positive rank curves due to this parity restriction using only the values of the character χ_d. As this character is ± 1 equally often, 50% of elliptic curves in a family of quadratic twists are even, and 50% are odd. This leads to the following famous open problem.

Conjecture 1 (Goldfeld)**.** *Families of quadratic twists of elliptic curves generically have 50% rank 0 curves and 50% rank 1 curves.*

In particular, we expect that about half of all square-free numbers n are congruent.

To give our promised test for when a number is congruent, we will actually encode the family of L-values $L(E_n, 1)$ using a single half-integral weight modular form. To do so, we will give a map

$$\{\text{ integral weight modular forms}\} \leftrightarrow \{\text{ half-integral weight modular forms}\}$$

where the half-integral weight modular forms "know" all L-values of the quadratic twists of their corresponding integral weight modular forms.

These maps were constructed by Shimura and Shintani, and the general results connecting to L-values follow from important work of Waldspurger. Next time, we'll start talking about a newer construction of Kohnen, which Kohnen and Kohnen-Zagier used to give an explicit form of Waldspurger's results convenient for our purposes.