Special values of L-functions of elliptic curves and modular forms

Notes by Tony Feng
for a talk by Chris Skinner

June 13, 2016

I'm going to begin by recalling a formula that Karl proved for the p-adic L-function of a CM elliptic curve. Then I'm going to describe some applications to the BSD conjecture, especially in the case of analytic rank 1.

1 A formula of Rubin

There are two main themes in the study of elliptic curves to date: Iwasawa theory and Heegner points. These two themes converge in Rubin's formula, which I'm not going to explain.

Let $E/\mathbb{Q}$ be an elliptic curve with CM by K. Then it has an associated Hecke character, which we denote by ψ_E, so that

$$L(E, s) = L(\psi_E, s).$$

There is a p-adic version of the Hecke character. Let p be a prime > 2, split in K. Write $p = v v^* = \mathfrak{p}\mathfrak{p}^*$. We get a Galois representation

$$\psi \colon G_K = \mathrm{Gal}(\overline{K}/K) \to \mathrm{Aut}_{\mathbb{Z}_p}(T_{\mathfrak{p}} E^\vee) \cong \mathbb{Z}_p^*$$

with Hodge-Tate weights $(1, 0)$. Then we get an identity(with the normalization geometric Frobenius)

$$L(\psi, s) = L(\psi_E, s).$$

Let $\Gamma = \mathrm{Gal}(K(E[p^\infty])/K)$. (This has rank 2 as a $\mathbb{Z}_p$-module, but also has torsion.) The characters ψ, ψ^* factor through Γ. Let $R = \widehat{\mathbb{Z}_p^{\mathrm{unr}}}$ and $\Lambda_R = R[[\Gamma]]$. Katz's 2-variable p-adic L-function $\mathcal{L}_v$ is an element of this ring.

For a continuous character

$$\phi \colon \Gamma \to \overline{\mathbb{Q}}_p^*$$

we denote

$$\widehat{\phi} \colon \Lambda_R \to \overline{\mathbb{Q}}_p$$

the induced map.

The p-adic L-function has the property that

$$\mathcal{L}_v(\phi) = \widehat{\phi}(\mathcal{L}_v).$$

This is the sense in which it interpolates classical Hecke characters.

Then

$$\mathcal{L}_v(\psi^k(\psi^*)^j, 0) = (*)L(\psi_E^k(\psi^*)^j, 0)\left(\frac{\Omega_p}{\Omega_\infty}\right)^{k-j}$$

for $k < 0$ and $j \geq 0$.

Theorem 1.1 (Rubin 1992)**.** *If* $\mathrm{ord}_{s=1} L(E, s) = 1$ *then there exists a* $y \in E(K)$ *of infinite order such that*

$$\mathcal{L}_v((\psi^*)^{-1}) = (*)(\log_{\omega_E} y)^2 \Omega_p^{-1}.$$

The explicit constant (*) can be expressed in terms of the p-part of Ш, etc. and lies in K^*.

Remark 1.2. One nice thing about this is that the logarithm detects points of finite/infinite order. We'll see that this formula is useful for exhibiting points of infinite order.

2 A formula of Bertolini-Darmon-Prasanna

Let $f \in \mathcal{S}_2^{\mathrm{new}}(\Gamma_0(N))$ for N square-free, say $f = \sum a_n q^n$. We write $\mathbb{C}(f) := \mathbb{C}(\{a_i\})$ and $\mathbb{Z}(f)$ for its ring of integers. Associated to such a modular form is an abelian variety A, and since we're interested in it only up to isogeny we can assume that the full ring of integers $\mathbb{Z}(f)$ acts on A.

Let K be an imaginary quadratic field such that the root number $\omega(H/K) = -1$. In this situation, we get a parametrization of our abelian variety by a Shimura curve X_B, meaning a uniformization

$$J(X_B) \to A$$

and also a Heegner point $y_K \in A(K)$. The natural question is: *is* y_K *of infinite order*?

Pick a prime $p \nmid 2N \,\mathrm{disc}(K)$, which is split in K. Write $p = vv^*$. Fix an embedding $\mathbb{C}(f) \hookrightarrow \overline{\mathbb{Q}}_p$, and let L be the completion of $\mathbb{C}(f)$ at the corresponding prime, and let O be its ring of integers.

The p-adic L-function. Let K_∞ be the anticyclotomic $\mathbb{Z}_p$-extension of K and $\Gamma = \mathrm{Gal}(K_\infty/K)$. Let $\Lambda = O[[\Gamma]]$ and $\Lambda_R = R[[\Gamma]]$, where $R = \widehat{O^{\mathrm{unr}}}$. There is a p-adic L-function $\mathcal{L}_v(f/K) \in R[[\Gamma]]$ with the property that if $\psi\colon G_K \to \Gamma \to \mathbb{C}_p^*$ which has Hodge-Tate weights $(-n, n), n > 0$ for the places (v, v^*) then

$$\mathcal{L}_v(f/K, \psi) = (*)L(f, \psi, 1) \cdot \left(\frac{\Omega_p}{\Omega_\infty}\right)^{4n}.$$

(The weight of the Grossencharacter is larger than that of the modular form, so it is the periods of ψ that show up rather than the periods of f.)

Theorem 2.1 (BDP/Brooks)**.** *We have*

$$\mathcal{L}_v(f/K, \chi_{triv}) = \left(\frac{1+p-a_p}{p}\right)^2 (\log_{\omega_f} y_K)^2.$$

To detect whether y_K is of finite order, we can try to compute the canonical height or the logarithm. The canonical height is, by Gross-Zagier, a value of the *derivative* of the L-function, and this theorem is telling us that the logarithm is a value of the L-function itself. This latter is easier to approach, e.g. via Iwasawa theory.

3 Iwasawa theory for $\mathcal{L}_v$

The Iwasawa theory of the usual anticyclotomic p-adic L-function has been studied by Darmon, Bertolini, ... by the anticyclotomic Euler system of Heegner points, and also by myself and Urban via the Eisenstein ideal.

Let V be the p-adic Galois representation over L associated to f (with the geometric normalization, so for f associated to an elliptic curve E it is the dual of the Tate module). Let $T \subset V$ be an $\mathcal{O}$-lattice.

Let $M = T^\vee \otimes_{\mathcal{O}} \Lambda^*$, which has the Galois action of $\rho_f \otimes \psi^{-1}$ where $\psi\colon G_K \twoheadrightarrow \Gamma \subset \Lambda^*$ is the natural quotient map. We consider the generalized Selmer group $\mathrm{Sel}_v(f/K) \subset H^1(K, M)$ with

- the usual local conditions away from p,
- no local condition at v
- the restriction at v^* must be 0.

Finally, set $X_v(f/K) = \mathrm{Sel}_v(f/K)^*$. This is a finitely generated Λ-module, which should be torsion.

Conjecture 3.1. *We have*

$$char_\Lambda(X_v(f/K)) = (\mathcal{L}_v(f/K))$$

as an equality in Λ_R.

Towards this conjecture we have the following result.

Theorem 3.2 (X. Wan)**.** *Suppose $p \geq 5$, T is residually irreducible, and at least $\ell \mid N$ is not split in K. Then $(\mathcal{L}_v(f/K)) \supset char_\Lambda(X_v(f/K))$ in $\Lambda_R \otimes \mathbb{Q}_p$.*

We can't use the usual Heegner hypothesis. Why not? Because we'll want to use Jacquet-Langlands transfer to a definite quaternion algebra.

We can extend this to an equality in Λ_R thanks to the following result.

Theorem 3.3 (Burungale)**.** *We have $\mu(\mathcal{L}_v(f/K)) = 0$.*

This direction is good for showing that $\mathcal{L}_v(f/K) \neq 0$, and hence that a p-adic logarithm doesn't vanish.

4 Converse to Gross-Zagier and Kolyvagin

Gross-Zagier/Kolyvagin show that if $\mathrm{ord}_{s=1} L(E/K, s) \leq r \leq 1$, then rank $E(K) = r$ and $\#Ш(E/K) < \infty$. We want to go in the other direction.

If rank $= 0$ and $\#Ш < \infty$ then this follows from my work with Urban on the Iwasawa main conjecture. I'm going to discuss the case of rank $= 1$ and $\#Ш < \infty$.

For concreteness, let's discuss elliptic curves instead of modular forms.

Theorem 4.1. *Assume (as is expected) that*

$$\begin{array}{ccc} \mathrm{Sel}_{p^\infty}(E/K) & \xrightarrow{\log} & E(K_v) \otimes \mathbb{Q}_p/\mathbb{Z}_p \\ \| & & \| \\ \mathbb{Q}_p/\mathbb{Z}_p \oplus \textit{finite} & & \mathbb{Q}_p/\mathbb{Z}_p \end{array}$$

is surjective. Then $\mathrm{ord}_{s=1} L(E/K, s) = 1$.

The idea is that one can use some Galois cohomology to show that $\#X_v(f/K)_\Gamma < \infty$. This comes from playing off the different conditions at p imposed on the Selmer group. That implies, by Wan's work, that $\mathcal{L}_v(f/K, \chi_{\mathrm{triv}}) \neq 0$. Then that implies by Bertolini-Darmon-Prasanna that y_K is non-torsion. Finally, use Gross-Zagier.

How might one check the hypothesis of the theorem (particularly surjectivity)?

Corollary 4.2. *Suppose*

$$\mathrm{Sel}_p(E/K) \cong \mathbb{Z}/p\mathbb{Z} \hookrightarrow \frac{E(K_v)}{pE(K_v) + E(K_v)[p]}.$$

Then $\mathrm{ord}_{s=1} L(E/K, s) = 1$.

At least in this result the hypothesis is a finite condition, which one can imagine could be checkable.

Remark 4.3. In joint work with Bhargava, we have results on counting elliptic curves that satisfy this condition. This allows us to show that there is a positive proportion of elliptic curves with analytic rank 1.

5 BSD formula

Theorem 5.1 (Jetcher-S-Wan)**.** *Let $E/\mathbb{Q}$ be semistable, $p \geq 5$ a prime of good reduction such that $E[p]$ is an irreducible $G_{\mathbb{Q}}$-representation. If* $\mathrm{ord}_{s=1} L(E, s) = 1$ *then*

$$\left| \frac{L'(E, 1)}{\Omega_E \cdot R_E} \right|_p = |\#Ш(E) \cdot \prod_{\ell | n_E} c_\ell|_p.$$

Remark 5.2. The novelty here is being able to handle the Tamagawa factors.

The idea is to look at what Gross-Zagier says about

$$\left|\frac{L'(E/K,1)}{\Omega_{E/K}\cdot R_{E/}}\right|_p$$

One gets that

$$\left|\frac{L'(E/K,1)}{\Omega_{E/K}\cdot R_{E/}}\right|_p = |\text{index of } y_K|_p^2$$

and by Galois cohomology we can relate the latter to $\log_E y_K$, which is related to Selmer groups. We can show that this is $\leq$ the expected value. Namely, since $L'(E/K,1) = L'(E/\mathbb{Q},1)L(E^K,1)$ and since we know Gross-Zagier in analytic rank 1 for E^K we can get the desired upper bound.

To get the lower bound we use an Euler system to bound the Tate-Shafarevich group. However, the Euler system argument loses information about the Tamagawa factors. The nice thing about Shimura curves is that, by making a right choice of imaginary quadratic field we can sweep the Tamagawa factors into degrees of parametrization so that Kolyvagin's argument actually becomes sufficient.

Let's go back to Corollary 4.2. How can we deal with the injectivity hypothesis? There is a "level-raising" idea exploited cleverly by Wei Zhang, but which goes back to Bertolini-Darmon. Find some modular form g of level $N_E\ell_1\ell_2$ (with ℓ_i inert in K) such that $f_e \equiv g$, and so that the Selmer group for g does satisfy the condition, has rank 1 and is non-zero at $v \mid p$. Then by geometric reciprocity laws, one deduces some non-vanishing of the original Heegner point at ℓ_1.

This furnishes the base case of an induction argument of Wei Zhang.

There was actually one final condition we didn't mention: we need that if $\ell \mid N_E$ and $\ell^2 \equiv 1 \mod p$ then $E[p]$ is ramified at ℓ.

Using these ideas, one can prove that Kato's main conjecture for his Euler system is true.