COMPUTATIONS OF SHA USING IWASAWA THEORY

CHRISTIAN WUTHRICH

Let $E/\mathbb{Q}$ be an elliptic curve. We wish to compute the p-primary part $Ш(E/\mathbb{Q})(p)$ of the Shafarevich-Tate group of E. Assume that p is an odd prime and that E has semistable reduction at p. For simplicity, in this talk, assume that the mod p reduction is ordinary (or multiplicative).

1. p-adic L-functions

Choose a generator $\gamma = 1 + p \in 1 + p\mathbb{Z}_p$. Then there is a canonical p-adic L-function $\mathcal{L}_p(E, T)$, where $T = \gamma^{s-1} - 1$, satisfying interpolation properties such as $\mathcal{L}_p(E, 0) = \text{something} \cdot L(E, 1)/\Omega_E^+$. It is computed by integrating against Mazur-Swinnerton-Dyer measure on $\mathbb{Z}_p^\times$.

Proposition 1.1. $\mathcal{L}_p(E, T) \in \mathbb{Z}_p[[T]]$ *(well known if $E[p]$ is irreducible, follows from Kato ...).*

2. p-adic BSD

Conjecture 2.1 (Mazur-Tate-Teitelbaum)**.**

- The order of vanishing of $\mathcal{L}_p(E, T)$ at $T = 0$ is $r = \operatorname{rank} E(\mathbb{Q})$, except in the "exceptional case" where E has split multiplicative reduction, in which case it is $r + 1$.
- The leading term is

$$\mathcal{L}_p^*(0) = b_p \frac{\prod c_v \# Ш(E/\mathbb{Q})}{(\# E(\mathbb{Q})_{\text{tors}})^2} \cdot \frac{\operatorname{Reg}_p(E/\mathbb{Q})}{\log(\gamma)^r} =: \operatorname{bsd}_p$$

  where
  - The c_v are Tamagawa numbers,
  - $\operatorname{Reg}_p(E/\mathbb{Q}) \in \mathbb{Q}_p$ is the canonical p-adic regulator
  -

$$b_p = \begin{cases} \left(1 - \frac{1}{\alpha}\right)^2 & \text{with } \alpha \text{ the unit eigenvalue of Frobenius} \\ \frac{h}{\log(\gamma)} = \frac{\log_p(q)}{\operatorname{ord}_p(q)\log(\gamma)}, & \text{if exceptional.} \end{cases}$$

3. Result from Iwasawa theory

Let X be the dual of the p^∞-Selmer group of E over the $\mathbb{Z}_p$-extension $\mathbb{Q}_\infty$ of $\mathbb{Q}$.

Kato: X is Λ-torsion and finitely generated where $\Lambda := \mathbb{Z}_p[[\Lambda]] \simeq \mathbb{Z}_p[[T]]$.

There is a characteristic series $f_X(T)$: There is a morphism $X \to \bigoplus_{i=1}^s \Lambda/f_i$ with finite kernel and cokernel; then $f_X(T) := \prod f_i(T)$.

The main conjecture: $f_X(T)$ (or $T f_X(T)$ in the exceptional case) is in $\mathcal{L}_p(E, T) \cdot \Lambda^\times$.

Date: June 5, 2007.

Kato: If $\rho_p\colon \operatorname{Gal}(\overline{\mathbb{Q}}/\mathbb{Q}) \to \mathrm{GL}_2(\mathbb{Z}_p)$ is surjective or if $E[p]$ is reducible, then $f_X(T)$ (or $Tf_X(T)$ in the exceptional case) divides $\mathcal{L}_p(E,T)$.

Perrin-Riou/Schneider/Jones: The order of vanishing of $f_X(T)$ is $\geq r$ (or $r+1$ in the exceptional case), with equality if and only if $\operatorname{Reg}_p(E/\mathbb{Q}) \neq 0$ and $Ш(E/\mathbb{Q})(p)$ is finite. If so, then $f_X^*(0) = \mathrm{bsd}_p$ up to multiplication by an element of $\mathbb{Z}_p^\times$.

4. Algorithms

We can compute an upper bound on $\operatorname{ord}_{T=0} \mathcal{L}_p(E/\mathbb{Q}) \geq \operatorname{ord}_{T=0} f_X(T) \geq r$. Suppose that $\operatorname{ord}_{T=0} \mathcal{L}_p(E/\mathbb{Q}) = r$, and suppose that we know $E(\mathbb{Q})$; then we can compute $\operatorname{Reg}_p(E/\mathbb{Q})$ and $\operatorname{ord}_p \mathcal{L}_p^*(E,0) \geq \operatorname{ord}_p f_X^*(0) = \operatorname{ord}_p(\mathrm{bsd}_p)$, and get $\operatorname{ord}_p Ш(E/\mathbb{Q})(p) \leq p$-adic analytic order of Ш.

Example 4.1. Let E be a semistable curve of rank 0. Then $\#Ш(E/\mathbb{Q})$ divides $2^{\text{something}} \frac{L(E,1)}{\Omega} \cdot \frac{(\#E(\mathbb{Q})_{\mathrm{tors}}))^2}{\prod c_v}$.