# A brief note on computing $p$-adic $L$-series of elliptic curves

Robert Pollack

February 3, 2007

## 1 Definition of $p$-adic $L$-series

Let $E/\mathbf{Q}$ be an elliptic curve. Fix $p$ a prime number. Denote by $\left[\frac{r}{s}\right]^+$ the positive modular symbol of $E$ associated to $\frac{r}{s}$ (defined up to choice of sign). Let $\alpha$ be a root of $x^2 - a_p x + p$ with $\mathrm{ord}_p(\alpha) < 1$. Here $a_p := p + 1 - E(\mathbf{F}_p)$. Such an $\alpha$ is unique in the ordinary case and is actually in $\mathbf{Z}_p^\times$. In the supersingular case, there are two choices for alpha both conjugate in a quadratic extension of $\mathbf{Q}_p$. Define a distribution on $\mathbf{Z}_p^\times$ by

$$\mu_{E,\alpha}^+(a + p^n\mathbf{Z}_p) = \frac{1}{\alpha^n}\left[\frac{a}{p^n}\right]^+ - \frac{1}{\alpha^{n+1}}\left[\frac{a}{p^{n-1}}\right]^+.$$

Then the $p$-adic $L$-series of $E$ is defined as a function on the $\mathbf{C}_p$-valued characters of $\mathbf{Z}_p^\times$ by integration with respect to $\mu_{E,\alpha}^+$. Here,

$$L_p(E,\alpha,\chi) = \int_{\mathbf{Z}_p^\times} \chi \; d\mu_{E,\alpha}^+$$

where $\chi : \mathbf{Z}_p^\times \to \mathbf{C}_p$ is a character.

## 2 Powers series expression for the $p$-adic $L$-series

Pick $\gamma$ a topological generator of $1+pZ_p$. Then characters of $1+pZ_p$ are defined uniquely by their value on $\gamma$. For $u \in \mathbf{C}_p$ with $|u-1|_p < 1$, define a character $\chi_u$ on $\mathbf{Z}_p^\times$ by first taking the natural projection of $\mathbf{Z}_p^\times$ onto $1 + pZ_p$ and then mapping $\gamma$ onto $u$.

The $p$-adic $L$-series $L_p(E,\alpha,\chi_u)$ is then analytic in the variable $u$ and we will denote its expansion about $u = 1$ by $L_{E,p,\alpha}(T) \in \mathbf{Q}_p(\alpha)[[T]]$. This power series is convergent on the open unit disc of $\mathbf{C}_p$. We have that

$$L_{E,p,\alpha}(u-1) = L_p(E,\alpha,\chi_u).$$

## 3 Explicit polynomial approximations of $L_{E,p,\alpha}(T)$

We can approximate $\int_{\mathbf{Z}_p^\times} \chi \, d\mu_{E,\alpha}^+$ via Riemann sums. The details of this calculation will not be done here. However, the end result is a sequence $L_n(T)$ of polynomials in $\mathbf{Q}_p(\alpha)[T]$ that converge to the $p$-adic $L$-series. Here,

$$L_n(T) = \sum_{j=0}^{p^{n-1}-1} \left( \sum_{a=1}^{p-1} \mu_{E,\alpha}^+ \left( \{a\}\gamma^j + p^n Z_p \right) \right) \cdot (1+T)^j$$

where $\{a\}$ is the Teichmuller lifting of $a$.

## 4 Computer calculations

The above formula for $L_n(T)$ allows one to readily approximate them on a computer. One can only approximate them as they have $Q_p(\alpha)$ coefficients.

In the ordinary case, $\alpha$ is in $\mathbf{Z}_p^\times$ and $L_n(T)$ should have $\mathbf{Z}_p$ coefficients. This is known when $E[p]$ is irreducible, but it is conjectured to happen generally. Analyzing the rate of convergence of the $L_n(T)$, one can see that it suffices to compute everything mod $p^n$ (taking care with possible $p$'s in the denominators of the modular symbols). Computing $\{a\}, \alpha$ and $(1+T)^j$ mod $p^n$ is very easy. All that is left to compute is $\left[\frac{a}{p^n}\right]^+$ and $\left[\frac{a}{p^{n-1}}\right]^+$ for $a$ prime to $p$ between 1 and $p^n$. This is the most time consuming part of the calculation.

In the supersingular case, $\alpha$ is in a quadratic extension of $\mathbf{Q}_p$ and $\mu_{E,\alpha}^+$ has $p$'s in its denominators on order about $p^{\frac{n}{2}}$. In this case $L_n(T)$ will not have $\mathbf{Z}_p$ coefficients. Nonetheless, no essential information is lost if one computes $\{a\}$ and $(1+T)^j$ only mod $p^n$. The end result should be that $L_n(T) = G_n(T) + H_n(T) \cdot \alpha$ with $G_n, H_n \in \mathbf{Q}_p[T]$ and scaling by $p^{\frac{n+2}{2}}$ will put both of them in $\mathbf{Z}_p[[T]]$.