Part 1. Modular symbols, $L$-values, and $\theta$-elements

1. Recall: Modular symbols
2. Recall: Modular symbols and $L$-values
3. Recall: $\theta$-elements and $\theta$-coefficients
4. $\theta$-elements for cyclic field extensions of prime order
5. The effect of the Atkin-Lehner involution on $\theta$-coefficients

Part 2. Statistics of modular symbols, theta-elements, and $L$-values

6. Distribution of modular symbols
7. Distribution of $\theta$-coefficients

References
that I took (with Karl Rubin’s permission) from a draft of a paper that Karl and I are writing.

1. **Recall: Modular symbols**

**Lemma 1.1.** In the discussion below, fix $E$ an elliptic curve over $\mathbb{Q}$ and let $N$ be the conductor of $E$. Let $\delta = \delta_E \in \mathbb{Z}_{>0}$ be the lcm of the orders of the torsion points in the Mordell-Weil group $E(\mathbb{Q})$.

For $r \in \mathbb{Q} \sqcup \{\infty\}$ we have:

(i) $[r]^\pm \in (2\delta)^{-1}\mathbb{Z}$,

(ii) $[\infty]^\pm = 0$,

(iii) $[r]^\pm = [r+1]^\pm$,

(iv) $[r]^\pm = \pm [-r]^\pm$,

(v) **Invariance:**

If

$$A := \begin{pmatrix} a & b \\ cN & d \end{pmatrix} \in \Gamma_0(N) \subset \text{SL}2(\mathbb{Z}),$$

so that for $r \in \mathbb{Q} \sqcup \{\infty\}$,

$$A(r) = (ar + b)/(cNr + d) \in \mathbb{Q} \sqcup \{\infty\},$$

we have the following relation in modular symbols:

$$[r]^\pm = [A(r)]^\pm - [A(\infty)]^\pm,$$

and if $A \in \Gamma_0(N)$, as automorphism of $H$, has a complex (quadratic) fixed point, then $[A(\infty)]^\pm = 0$, and therefore:

$$[A(r)]^\pm = [r]^\pm$$

for all $r \in \mathbb{Q} \sqcup \{\infty\}$,

(vi) **Atkin-Lehner relation:** Suppose $m \geq 1$ and write $N = ef$ where $f := \gcd(m,N)$. If $a, d \in \mathbb{Z}$, and $ade \equiv 1 \pmod{m}$, and $w_e$ is the eigenvalue of the Atkin-Lehner operator $W_e$ on $f_E$, then

$$[d/m]^\pm = -w_e \cdot [a/m]^\pm,$$

(vii) **Hecke relations:** Suppose $\ell$ is a prime, and $a_\ell$ is the $\ell$-th Fourier coefficient of $f_E$.

(a) If $\ell \nmid N$, then $a_\ell \cdot [r]^\pm = [\ell r]^\pm + \sum_{i=0}^{\ell-1}[(r+i)/\ell]^\pm$. 
(b) If $\ell \mid N$, then $a_\ell \cdot [r]^\pm = \sum_{i=0}^{\ell-1} [(r + i)/\ell]^\pm$.

Proof. The proofs of (i)—(v) are evident. For (vi), here is a construction of the Atkin-Lehner operator $W_e$. Let $f = \gcd(m, N)$ and $N = ef$. The $W_e$ operator is given by (any) matrix of the following form:

$$W_e := \begin{pmatrix} a & b \\ cN & de \end{pmatrix},$$

with $a, b, c, d \in \mathbb{Z}$ and $\det(W_e) = e$.

Let $c = m/f$. Then (since $e$ and $f$ are relatively prime) we can find $a$ and $b$ to make a matrix of the desired form, and then

$$W_e(\infty) = ae/cN = a/cf = a/m,$$

and (computing)

$$W_e(d/m) = \infty$$

Thus $W_e$ takes the path $\{\infty, d/m\}$ to the path $\{a/m, \infty\}$. It follows that $[d/m] = -w_E[a/m]$ where $w_E$ is the eigenvalue of $W_e$ acting on the newform uniformizing $E$, and $ade \equiv 1(\text{mod } f)$ (the latter because $\det(W_e) = e$).

The proof of (vii) is straightforward. \(\Box\)

Remarks 1. (i) A random example: For the elliptic curve $E := \text{“11a”}$ (aka: $X_0(11)$) here are the values of $[a/13]^+_E$.

- $[0]^+_E = 1/5$,
- $[1_{13}]^+_E = -4/5$,
- $[2_{13}]^+_E = [3_{13}]^+_E = 17/10$,
- $[4_{13}]^+_E = [5_{13}]^+_E = [6_{13}]^+_E = -4/5$.

Note that $X_0(11)$ has a rational point of order 5, so $\delta = 5$; hence the denominators of the values are multiples of $2\delta = 10$. If you believe BSD and the Shafarevich-Tate conjecture the $1/5$ already tells us (the true fact!) that the Mordell-Weil
group of $X_0(11)$ is of order 5 and the Shafarevitch-Tate group is trivial.

(ii) SAGE conveniently computes modular symbols data (for a hint of this, see W. Stein’s \[\text{http://doc.sagemath.org/html/en/reference/modsym/sage/modular/modsym/modular_symbols.html}\].

(iii) Note that as in Chi-Yun’s lecture, the computation of modular symbols via “Manin symbols” follows the route of a continued fractions (i.e., Euclidean algorithm-type) reduction so one gets a qualitative (“log”) upper bound for the size of modular symbols:

$$\left|\left[a/m\right]^\pm\right| \ll \log(m).$$

(iv) The Hecke relation vii(a) above applied to a prime $\ell \nmid N$, and $r = 0$ gives us

$$\begin{equation}
(a_\ell - 1) \cdot [0]^+ = \sum_{i=0}^{\ell-1} [i/\ell]^+ = L(E, 1)/\Omega^+
\end{equation}$$

and moving one “$[0]^+$” from right to left in 1.2 and switching sides we get:

$$\begin{equation}
\sum_{i=1}^{\ell-1} [i/\ell]^+ = (a_\ell - 2) \cdot [0]^+
\end{equation}$$

Proceeding similarly by induction, we have:

**Proposition 1.4.** Let $m = \prod_{j=1}^{\nu} \ell_j$ be square free (the $\ell_j$ being distinct primes) and prime to $N$, then:

$$\begin{equation}
\sum_{(i,m)=1; \ i \leq m} [i/m]^+ = \prod_{j=1}^{\nu} (a_{\ell_j} - 2) \cdot [0]^+
\end{equation}$$
2. Recall: Modular symbols and \(L\)-values

**Definition 2.1.** Suppose \(\chi\) is a primitive Dirichlet character of conductor \(m\). Define the Gauss sum
\[
\tau(\chi) := \sum_{a=1}^{m} \chi(a)e^{2\pi ia/m}
\]
and, if \(L(E, s) = \sum a_n n^{-s}\), the twisted \(L\)-function
\[
L(E, \chi, s) := \sum_{n=1}^{\infty} \chi(n)a_n n^{-s}.
\]

If \(F/\mathbb{Q}\) is a finite abelian extension of conductor \(m\), we will identify characters of \(\text{Gal}(F/\mathbb{Q})\) with primitive Dirichlet characters of conductor dividing \(m\) in the usual way.

**Proposition 2.2.** If \(F/\mathbb{Q}\) is a finite abelian extension, then
\[
L(E_{/F}, s) = \prod_{\chi: \text{Gal}(F/\mathbb{Q}) \to \mathbb{C}^\times} L(E, \chi, s).
\]

**Corollary 2.3.** If the Birch and Swinnerton-Dyer conjecture holds for \(E_{/\mathbb{Q}}\) and \(E_{/F}\), then
\[
\text{rank}(E(F)) = \text{rank}(E(\mathbb{Q})) + \sum_{\chi: \text{Gal}(F/\mathbb{Q}) \to \mathbb{C}^\times} \text{ord}_s L(E, \chi, s).
\]

**Theorem 2.4 (Birch-Stevens).** If \(\chi\) is a primitive Dirichlet character of conductor \(m\), then
\[
\sum_{a=1}^{m} \chi(a)[a/m]^{\epsilon} = \frac{\tau(\chi)L(E, \bar{\chi}, 1)}{\Omega_E^+}.
\]
where the sign \(\epsilon\) is equal to the sign of the character \(\chi\), i.e., \(\epsilon = \chi(-1)\).

**Remark:** This also works for the trivial primitive character applied to the element \(r = 0 \in \mathbb{P}^1(\mathbb{Q})\):
\[
(2.5) \quad [0]^+ = L(E, 1)/\Omega_E^+.
\]

(so the vanishing of \(L(E, s)\) at \(s = 1\) is equivalent to \([0]^+ = 0\).
3. Recall: $\theta$-elements and $\theta$-coefficients

**Definition 3.1.** Suppose $m \geq 1$, and let $G_m = \text{Gal}(\mathbb{Q}(\mu_m)/\mathbb{Q})$. Identify $G_m$ with $(\mathbb{Z}/m\mathbb{Z})^\times$ in the usual way, and let $\sigma_{a,m} \in G_m$ be the Galois automorphism corresponding to $a \in (\mathbb{Z}/m\mathbb{Z})^\times$ (i.e., $\sigma_{a,m}$ acts on $\mu_m$ as raising to the $a$-th power). Define

$$
\theta_m^\pm := 2\delta \sum_{a \in (\mathbb{Z}/m\mathbb{Z})^\times} [a/m]^\pm \sigma_{a,m} \in \mathbb{Z}[G_m].
$$

If $F/\mathbb{Q}$ is a finite abelian extension of conductor $m$, so $F \subset \mathbb{Q}(\mu_m)$, define the $\theta$-element (over $F$, associated to $E$) to be:

$$
\theta_F^\pm := \theta_m^\pm|_F \in \mathbb{Z}[\text{Gal}(F/\mathbb{Q})]
$$

where $\theta_m^\pm|_F$ is the image of $\theta_m^\pm$ under the natural restriction homomorphism

$$
\mathbb{Z}[\text{Gal}(\mathbb{Q}(\mu_m)/\mathbb{Q})] \to \mathbb{Z}[\text{Gal}(F/\mathbb{Q})].
$$

**Note:** We probably should denote $\theta_F$ as $\theta_{F/\mathbb{Q}}$ to emphasize that the base field here is $\mathbb{Q}$. An interesting project is to develop and possibly find algorithms for computing the analogous ‘$\theta$-elements,’ $\theta_{F/K}$ for cyclic Galois extensions $F/K$ where $K$ is a more general number field. There is such a theory of ‘$\theta$-elements’ (gotten by reverse-engineering the appropriate generalization of Theorem 2.4); and conjecturally $\theta_{F/K} \in \mathbb{Z}[\text{Gal}(F/K)] \subset \mathbb{C}[\text{Gal}(F/K)]$.

By Lemma 1.1(i) we have

$$
(3.2) \quad \theta_F^\pm = \sum_{\gamma \in \text{Gal}(F/\mathbb{Q})} c_{F,\gamma}^\pm \cdot \gamma \in \mathbb{Z}[\text{Gal}(F/\mathbb{Q})]
$$

where

$$
(3.3) \quad c_{F,\gamma}^\pm = 2\delta \cdot \sum_{a \text{ (mod } m)} [a/m]^\pm.
$$

We will refer to the $c_{F,\gamma}^\pm \in \mathbb{Z}$ as $\theta$-coefficients. Since we will most often be dealing with the ‘plus’$\theta$-elements, we will simplify notation by letting $\theta_F := \theta_F^+$, $c_{F,\gamma} := c_{F,\gamma}^+$, and $\Omega := \Omega^+$. If $F$ is a real field, then $\sigma_{-1,m}|_F = 1$, so

$$
(3.4) \quad c_{F,\gamma} = 2\delta \cdot \sum_{a \in (\mathbb{Z}/m\mathbb{Z})^\times/\{\pm 1\}} [a/m].
$$
Remark: From the definition \(3.3\) we have
\[
\sum_{\gamma \in \text{Gal}(F/Q)} c_{F,\gamma} = 4\delta \cdot \sum_{i \in \mathbb{Z}/m\mathbb{Z}^\times /\{\pm 1\}} [i/m].
\]
and therefore by Proposition \(1.4\) if \(m = \prod_{j=1}^{\nu} \ell_j\) is squarefree and prime to \(N\), we have:
\[
\sum_{\gamma \in \text{Gal}(F/Q)} c_{F,\gamma} = 4\delta \cdot \prod_{j=1}^{\nu} (a_{\ell_j} - 2) \cdot [0]^+. \tag{3.6}
\]

Proposition \(2.4\) can be rephrased as follows:

**Corollary 3.7.** Suppose \(F/Q\) is a finite real cyclic extension of conductor \(m\) and \(\chi : (\mathbb{Z}/m\mathbb{Z})^\times \rightarrow \text{Gal}(F/Q) \hookrightarrow \mathbb{C}^\times\) is a character that cuts out \(F\). Then
\[
\bar{\chi}(\theta_F) = 2\delta \cdot \frac{\tau(\bar{\chi}) L(E, \chi, 1)}{\Omega_E}. \tag{3.8}
\]

4. \(\theta\)-elements for cyclic field extensions of prime order

(i) Let \(\chi\) be a character of order a prime number \(p > 2\) and of squarefree conductor \(m = \prod_{j=1}^{\nu} \ell_j\) relatively prime to \(N\), so \(p \mid \phi(m)\) and then (by Equation \(3.2\))
\[
\bar{\chi}(\theta_F) = \sum_{\gamma \in \text{Gal}(F/Q)} c_{F,\gamma}^+ \cdot \bar{\chi}(\gamma) \in \mathbb{Z}[e^{2\pi i/p}].
\]

If \(\gamma_0 \in \text{Gal}(F/Q)\) is a generator of the group \(\text{Gal}(F/Q)\), putting \(\zeta_p := \bar{\chi}(\gamma_0)\) we can write the above equation as:
\[
\bar{\chi}(\theta_F) = \sum_{i=0}^{p-1} c_{F,\gamma_0^i}^+ \cdot \zeta_p^i \in \mathbb{Z}[e^{2\pi i/p}].
\]

So, the vanishing of \(\bar{\chi}(\theta_F)\) (equivalently: of \(L(E, \chi, 1)\)) occurs if and only if all the \(c_{F,\gamma}^+\) are equal. Recalling:
\[
\sum_{\gamma \in \text{Gal}(F/Q)} c_{F,\gamma} = 4\delta \cdot \prod_{j=1}^{\nu} (a_{\ell_j} - 2) \cdot [0]^+. \tag{4.1}
\]
we get:
Proposition 4.2. Let $\chi$ be a character of order a prime number $p > 2$ and of squarefree conductor $m = \prod_{j=1}^{\nu} \ell_j$ relatively prime to $N$, cutting out the Galois cyclic field extension $F/\mathbb{Q}$ (of order $p$) then the following are equivalent:

(a) $\chi(\theta_F) = 0$,

(b) $L(E, \chi, 1) = 0$,

(c) For all $\gamma \in \text{Gal}(F/\mathbb{Q})$

\[
c_{F,\gamma} = \frac{4\delta}{p} \prod_{j=1}^{\nu} (a_{\ell_j} - 2) \cdot [0]^+.
\]

(ii) Example: $E := X_0(11)$ over $\mathbb{Q}$

The Mordell-Weil group of $E$ is cyclic of order 5. So $\delta = 5$. Also (see Remark [1] above) we have $[0]^+_E = \frac{1}{5}$.

So if $\chi$ satisfies the hypotheses of Proposition 4.2 and if $L(E, \chi, 1) = 0$, Equation 4.3 above would read:

\[
c_{F,\gamma} = \frac{4}{p} \prod_{j=1}^{\nu} (a_{\ell_j} - 2).
\]

and since $c_{F,\gamma} \in \mathbb{Z}$ this would force

\[a_{\ell_j} \equiv 2 \mod p\]

for at least one $j = 1, 2, \ldots, \nu$. That is, we have the converse:

If $\chi$ satisfies the hypotheses of Proposition 4.2 then

\[a_{\ell_j} \not\equiv 2 \mod p, \text{ for all } j \leq \nu \implies L(E, \chi, 1) \neq 0.\]

Discuss the corresponding issues with Selmer.

5. THE EFFECT OF THE ATKIN-LEHNER INVOLUTION ON $\theta$-COEFFICIENTS

Definition 5.1. Suppose $F$ is a finite real cyclic extension of $\mathbb{Q}$, let $m$ be its conductor, and let $f = \gcd(m, N)$ where $N$ is the conductor of $E$ and assume that $f$ is relatively prime to $e := N/f$. Let $\gamma_F$ be the image of $e$ under the map

\[(\mathbb{Z}/m\mathbb{Z})^\times \to \text{Gal}(F/\mathbb{Q}).\]
Define an involution $\iota_F$ of the set $\text{Gal}(F/Q)$ by

$$\iota_F(\gamma) = \gamma^{-1} \gamma_F^{-1}.$$ 

Recall that $\theta_F = \sum_{\gamma \in \text{Gal}(F/Q)} c_{F,\gamma} \gamma$. 

**Lemma 5.2.** Suppose $F$ is a finite real cyclic extension of $Q$.

(i) We have

$$c_{F,\gamma} = -w_e c_{F,\gamma'}$$

where $\gamma' := \iota_F(\gamma) = \gamma^{-1} \gamma_F^{-1}$ and where $w_e$ is the eigenvalue of the Atkin-Lehner operator $W_e$ acting on $f_E$.

(ii) The fixed points of $\iota_F$ are the square roots of $\gamma_F^{-1}$ in $\text{Gal}(F/Q)$, so the number of fixed points is:

- one if $[F : Q]$ is odd,
- zero if $\gamma_F$ is not a square in $\text{Gal}(F/Q)$,
- two if $[F : Q]$ is even and $\gamma_F$ is a square in $\text{Gal}(F/Q)$.

(iii) If $\gamma = \iota_F(\gamma)$ and $w_e = 1$, then $c_{F,\gamma} = 0$.

**Proof.** Assertion (a) follows from the Atkin-Lehner relations satisfied by the modular symbols (Lemma 1.1(iv)). Assertion (b) is immediate from the definition, and (c) follows directly from (a). □

**Definition 5.3.** If $F/Q$ is a real cyclic extension, we say that $\gamma \in \text{Gal}(F/K)$ is generic, (resp., special+, resp., special−) if $\gamma \neq \iota_F(\gamma)$ (resp., $\gamma = \iota_F(\gamma)$ and $w_e = -1$, resp., $\gamma = \iota_F(\gamma)$ and $w_e = 1$).

By Lemma 5.2(iii), if $\gamma$ is special− then $c_{F,\gamma} = 0$.

**Part 2. Statistics of modular symbols, theta-elements, and $L$-values**

6. **Distribution of modular symbols**

The following fundamental result about the distribution of modular symbols was proved by Petridis and Risager (cf. (8.6) of [4]). For simplicity, we will formulate these results only if the conductor $N$ of $E$ is squarefree (even though their results are more general).

**Definition 6.1.** Let $C_E := 6/\pi^2 \prod_{p \mid m} (1 + p^{-1})^{-1} \cdot L(\text{Sym}^2(E), 2)$. 


Theorem 6.2 (Petridis & Risager [4]). As $X$ goes to infinity the values
\[ \left\{ \frac{[a/m]^+}{\sqrt{\log(m)}} : m \leq X, a \in (\mathbb{Z}/m\mathbb{Z})^\times \right\} \]
approach a normal distribution with variance $C_E$.

Numerical experiments led to the following conjecture. Denote by $\text{Var}(m)$ the variance
\[ \text{Var}(m) := \frac{1}{\varphi(m)} \sum_{a \in (\mathbb{Z}/m\mathbb{Z})^\times} ([a/m]^+)^2 \]

Conjecture 6.3. 
(i) As $m$ goes to infinity, the distribution of the sets
\[ \left\{ \frac{[a/m]^+}{\sqrt{\log(m)}} : a \in (\mathbb{Z}/m\mathbb{Z})^\times \right\} \]
converge to a normal distribution with mean zero and variance $C_E$.
(ii) For every divisor $\kappa$ of the conductor $N$, there is a constant $D_{E,\kappa} \in \mathbb{R}$ such that
\[ \lim_{m \to \infty} (\text{Var}(m) - C_E \log(m)) = D_{E,\kappa}. \]

Note that Theorem 6.2 is an “averaged” version of Conjecture 6.3(i). Inspired by Conjecture 6.3, Petridis and Risager [5, Theorem 1.6] obtained the following result, which identifies the constant $D_{E,\kappa}$ and proves an averaged version of Conjecture 6.3(ii).

Theorem 6.4 (Petridis & Risager [5]). We continue to suppose that $N$ is squarefree. For every divisor $\kappa$ of $N$, there is an explicit (see [5, (8.12)]) constant $D_{E,\kappa} \in \mathbb{R}$ such that
\[ \lim_{X \to \infty} \frac{1}{\varphi(m)} \sum_{m \leq X \atop (m,N) = \kappa} \varphi(m)(\text{Var}(m) - C_E \log(m)) = D_{E,\kappa}. \]

(Yesterday) I also received a very new preprint by Junwong Lee and Hae-Sung Sun Dynamics of Continued Fractions and Distribution of Modular Symbols with a very different proof of these results. (I have the permission of the authors to put it on the course web-page—which I’ll do.)
6.1. The ‘irrelevant’ nonrandomness of the modular symbols.

Remark 6.5. The modular symbols are not completely “random” subject to Conjecture 6.3. Specifically partial sums $\sum_{a=\alpha}^{\beta} [a/m]$ behave in a somewhat orderly way—even though it seems only to be the full sum that affects the statistics of $\theta$-coefficients. Numerical experiments led the authors and William Stein to propose the following conjecture.

Conjecture 6.6. If $0 < x < 1$ then

$$\lim_{m \to \infty} \frac{1}{m} \sum_{a=1}^{\infty} \frac{a/n \sin(\pi n x)}{n^2 \Omega_E}$$

where $\sum_n a_n q^n$ is the modular form $f_E$ corresponding to $E$.

This conjecture was recently proved for prime denominators by Kim and Sun [3, Theorem A].

Theorem 6.7 (Kim & Sun [3]). If $0 < x < 1$ then

$$\lim_{m \to \infty} \frac{1}{m} \sum_{a=1}^{m} [a/m] = \sum_{n=1}^{\infty} \frac{a_n \sin(\pi n x)}{n^2 \Omega_E}.$$ 

7. Distribution of $\theta$-coefficients

By [3.4], if $\gamma$ is generic (resp., special+) then the theta coefficient $c_{F,\gamma}$ is twice a sum of $\varphi(m)/(2[F : \mathbb{Q}])$ modular symbols (resp., four times a sum of $\varphi(m)/(4[F : \mathbb{Q}])$ modular symbols). If these were randomly chosen modular symbols, one would expect from Conjecture 6.3(i) that these coefficients would have a normal distribution with variance $2C_E \varphi(m) \log(m)/[F : \mathbb{Q}]$ (resp., variance $4C_E \varphi(m) \log(m)/[F : \mathbb{Q}]$).

However, calculations do not support this expectation. Instead, they support the following conjecture—which our hope is to eventually make a good deal more precise!

For every $d > 2$, let $\Sigma_d$ denote the collection of data

$$\Sigma_d := \left\{ \frac{c_{F,\gamma} \sqrt{d}}{\sqrt{\varphi(m) \log(m)}} : F/\mathbb{Q} \text{ real, cyclic of degree } d, \right.$$ 

$$m = \text{cond}(F), \quad \gamma \in \text{Gal}(F/\mathbb{Q}) \text{ generic} \right\},$$

ordered by $m$. Let $\Sigma_d^+$ be defined in the same way, for $\gamma$ special+ instead of generic.
Conjecture 7.1. For every \( d \geq 2 \), the collections of data \( \Sigma_d \) and \( \Sigma_d^+ \), ordered by \( m \), have limiting distributions \( \Lambda_{E,d}(t) \) and \( \Lambda_{E,d}^+(t) \). As \( d \) grows, \( \Lambda_{E,d}(t) \) (resp., \( \Lambda_{E,d}^+(t) \)) converges to a normal distribution with variance \( 2C_E \) (resp., \( 4C_E \)).

Question 7.2. Is it the case that for \( d \gg 0 \) \( \Lambda_{E,d}(t) \) and \( \Lambda_{E,d}^+(t) \) are continuous bounded functions?

References


