1. Math 258: L-Functions and Arithmetic Statistics

The format of this "topics course" Math 258 will consist of some lectures from me (and possibly other faculty and guests) but I hope it will *mainly* be composed of student lectures. Even though the title of our course is *L-Functions and Arithmetic Statistics*, the aim is to understand as best we can the nature of rational points on algebraic curves—both statistics related to this and explicit methods of computation.

There are no exams in this course—the only requirements will be **(a)** participation in general and **(b)** specifically: to give one or two lectures on a topic germane to one of the three the general areas related to modular symbols and arithmetic described below. The focus will be background to appreciate some of the current work in this area—e.g., in arithmetic statistics, Chabauty's technique and its very recent elaborations, and Selmer groups. How much time, we spend on any of these areas will depend on the preference of the participants.

Here, then, is the general spread of our topics:

Modular symbols $\longrightarrow$ **Θ-elements** $\longrightarrow$

$\longrightarrow$ **Special values of L-functions** $\longrightarrow$ **L-functions** $\longrightarrow$

$\xrightarrow{\text{conjecture}}$

$\longrightarrow$ **Selmer groups or varieties** $\longrightarrow$ **Rational points**

I.e.,

Combinatorics $\longrightarrow$ **Analysis** $\longrightarrow$ **Algebraic number theory and geometry** $\longrightarrow$ **Arithmetic**

2. General comments

How many rational points are there? Theorems, Conjectures, Statistics:

Since we've been trying—for millennia—to understand phenomena related to rational points (of curves or of varieties of various types) it's of interest to take stock of current work (proved, or conjectured) regarding general statistical features of these phenomena; and to study whatever new developments—either proved or conjectured—that there are for actual computation and determination (e.g., of these statistics, and of the rational points themselves).

Conjectures (and some results) suggest that, on the whole, algebraic varieties over a number field K tend not to have all that many K-rational points unless either

- there is some specific algebraic geometric structure (e.g., a group structure in the works) generating them,

or, in the case, say, of abelian varieties

- a functional equation (proved, or conjectured) and a corresponding root number computation predicts the parity of the rank of a Mordell-Weil group (which in many cases allows one to expect the existence of more rational points than is in evidence without this prediction).

But lacking either reason for rational points to be abundant[1] , the sense is that they are scarce.

For curves, there is recent work that emphasizes the scarcity of points. For example, the body of work of Manjul Bhargava and his collaborators offer (*proved*) results indicating, in general terms, that statistically we may expect few rational points in various contexts; e.g., the work of Manjul Bhargava, Benedict H. Gross, and Xiaoheng Wang may be roughly interpreted as showing that most hyperelliptic curves of high genus have relatively few rational points (*Pencils of quadrics and the arithmetic of hyperelliptic curves*: http://arxiv.org/abs/1310.7692).

One also has classical results stemming from Chabauty's method such as Robert Coleman's corollary (in *Effective Chabauty*, Duke Math. J. **52** (1985), no. 3, 765-770) that any curve over $\mathbb{Q}$ of genus 2 with

[1] A conjecture of Lang implies that a variety over a number field has infinitely many rational points only if it contains a rational curve or a nontrivial image of an abelian variety.

good reduction at 2 or 3 and the Mordell-Weil rank of its jacobian ≤ 1 possesses at most 12 $\mathbb{Q}$-rational points.

How many rational points are there? Heuristics:

Moreover, various different *types of heuristics* play a role in leading us to expect further manifestations of 'scarcity.' For example:

- For elliptic curves, the remarkable guess (originally made by Honda for families of quadratic twists of a single elliptic curve) that there is a finite upper bound to the Mordell-Weil ranks of all elliptic curves over $\mathbb{Q}$ has been given some support by heuristics developed in the article *A heuristic for boundedness of ranks of elliptic curves*[2]. The heuristic set-up here connects to the earlier 'Cohen-Lenstra' heuristic regarding ideal class groups. The conjecture, by the way, is that this maximal rank is not only finite, but quite small.

- David, Fearnley, and Kisilevsky (DFK) make use of *random matrix heuristics* to (essentially[3]) conjecture that if E is an elliptic curve over $\mathbb{Q}$ for any prime number $p > 5$ there are only finitely many cyclic extensions K of $\mathbb{Q}$ such that $E(K)$ is strictly larger than $E(\mathbb{Q})$. (This connects with the question of *Diophantine stability* for more general curves and varieties[4], a topic that we want to consider in this seminar-course.)

- Inspired by (DFK), Karl Rubin and I have been framing conjectures (and proving some theorems) and making some computations regarding modular symbols to develop a somewhat more naive heuristic format in hopes that it gives the same qualitative conclusion as DFK. Curiously—although the qualitative predictions are the same—at the moment there are very slight (power of log) differences in certain instances between this heuristic and the more sophisticated random matrix heuristic; we hope to understand this better.

---

[2] J. Parks, B. Poonen, J. Voight, M. Wood arXiv:1602.01431v3

[3] They actually conjecture the corresponding statement for nonvanishing of special values of the relevant L-functions.

[4] A variety V over a field K is saidto be **Diophantine stable** for the field extension L/K if V 'acquires no new rational points' under the base change from K to L; i.e., if $V(L) = V(K)$.

How many rational points are there? Theorems. Specific computations:

We will have presentations about new results regarding Selmer groups (which allow us to use Galois cohomology to control the size of the rank of the Mordell-Weil group of abelian varieties) and regarding Selmer *varieties* which occur in the method of Chabauty-Coleman-Kim. This new approach has been used[5] to compute rational points of curves in cases that were beyond the reach of older methods[6].

3. Basic references

(i) **Modular symbols, θ-elements and L-functions.**

(a) The basics
(b) Some statistics
(c) Applications to theorems (and conjectures) regarding rational points.

A few relevant references:

- S. Lang, Introduction to Modular Forms, Springer-Verlag (Chapters IV, V) `https://wstein.org/edu/Fall2003/252/references/lang-intro_modform/Lang-Introduction_to_modular_forms.pdf`
- J. I. Manin, Parabolic points and zeta functions of modular curves, Izv. Akad. Nauk SSSR Ser. Mat. 36 (1972), 19-66. `https://wstein.org/edu/Fall2003/252/references/Manin-Parabolic/Manin-Parabolic_points_and_zeta_functions_of_modular_curves.pdf`
- B. Mazur, Courbes elliptiques et symboles modulaires, Séminaire Bourbaki, 24‘eme année (1971/1972), Exp. No. 414, Springer, Berlin, 1973, pp. 277- 294. Lecture Notes in Math., Vol. 317.
- B. Mazur-K. Rubin (to be specified; various articles)
- Y. N. Petridis, M.S. Risager, Arithmetic statistics of modular symbols, arXiv:1703.09526

[5] by J. S. Balakrishnan, N, Dogra, J.S. Müller, J. Tuitman, J. Vonk, and *by people in this seminar*

[6] Among these are *some of the* the (very interesting) curves $X = X_0(p)^+$ for p prime.

- W. Stein, Modular Forms, a Computational Approach, AMS https://wstein.org/books/modform/stein-modform.pdf (Chapter 3, especially and Chapter 8)
- W. Stein, Statistics of modular symbols: https://sites.math.washington.edu/~bviray/NTS/SteinApril7.pdf
- W. Stein,Introduction to modular symbols, https://wstein.org/edu/Fall2003/252/lectures/09-26-03/intro_to_modular_symbols.pdf

(ii) **Selmer groups**

(a) The basics
(b) Results about statistics
(c) Applications—especially to theorems regarding rational points, and (perhaps) Diophantine Stability.

A few relevant references:

- M. Stoll, Selmer groups and Descent https://people.maths.bris.ac.uk/~matyd/Trieste2017/Stoll.pdf
- B. Poonen, Selmer group heuristics http://math.mit.edu/~poonen/papers/aws2014.pdf
- M. Bhargava, D. Kane, H. Lenstra, B. Poonen, E. Rains, Modeling the distribution of ranks, Selmer groups, and Shafarevitch-Tate groups of elliptic curves, https://math.mit.edu/~poonen/papers/rst_distribution.pdf
- Z. Djabri, E. F. Schaefer, N.P. Smart, Computing the p-Selmer group of an elliptic curve http://www.hpl.hp.com/techreports/98/HPL-98-178R1.pdf
- B. Mazur, K. Rubin, M. Larsen, Diophantine Stability, https://arxiv.org/abs/1503.04642

(iii) **Rational points**

(a) some basics, but on to:
(b) Chabauty's method and its refinements.

A few relevant references:

- (A "learning seminar" for nonabelian Chabauty run by Bjorn Poonen at MIT): http://math.mit.edu/nt/old/stage_s18.html
- W. McCallum, B. Poonen The method of Chabauty and Coleman http://www-math.mit.edu/~poonen/papers/chabauty.pdf
- M. Kim, The motivic fundamental group of P1 0, 1, and the theorem of Siegel, http://people.maths.ox.ac.uk/kimm/papers/siegelinv.pdf
- M. Kim, The Unipotent Albanese Map and Selmer Varieties for Curves, http://people.maths.ox.ac.uk/kimm/papers/alb.pdf
- J. S. Balakrishnan, N, Dogra Quadratic Chabauty and rational points I: p-adic heights https://arxiv.org/abs/1601.00388
- J. S. Balakrishnan, N, Dogra, Quadratic Chabauty and rational points II: Generalised height functions on Selmer varieties, https://arxiv.org/abs/1705.00401
- J. S. Balakrishnan, N, Dogra, J.S. Müller, J. Tuitman, J. Vonk, Explicit Chabauty-Kim for the split Cartan modular curve of level 13 http://people.maths.ox.ac.uk/vonk/documents/p_cartan.pdf
- B. Lawrence, A.Venkatesh, Diophantine problems and p-adic period mappings arxiv.org/abs/1807.02721

modsymb0

Part 1. Modular symbols

4. Digression: 'pre-modular symbols'

As an introduction to modular symbols, we might recall that such symbols arise from the structure of uniformization of Riemann surfaces, hyperbolic metrics and geodesics:

- Discuss the basic hyperbolic structure; i.e., $\mathbf{H}$:= the upper half plane and its ' completion,'

$$\bar{\mathbf{H}} := \mathbf{H} \sqcup \mathbf{P}^1(\mathbb{Q}) \subset \mathbb{C}.$$

  Let Γ be a discrete (congruence) subgroup of $\mathrm{PSL}_2(\mathbb{Z})$ so that Γ acts on $\mathbf{H}$ and $\bar{\mathbf{H}}$.

  Passing to quotients, put

$$u : \mathbf{H} \to Y := \mathbf{H}/\Gamma,$$

$$\bar{u} : \bar{\mathbf{H}} \to X = Y \sqcup \mathcal{C},$$

  where

$$\mathcal{C} := \mathbf{P}^1(\mathbb{Q})/\Gamma = \text{ the cusps.}$$

- Define, for $a/b \in \mathbf{P}^1(\mathbb{Q}) = \mathbb{Q} \cup \{\infty\}$, the element

$$\ll a/b, c/d \gg \quad \in \quad \pi_1(X, \mathcal{C})$$

  to be the image of the geodesic in $\mathbf{H}$ with endpoints $a/b, c/d \in \mathbf{P}^1(\mathbb{Q})$ (and oriented as going from a/b to c/d) in this *relative fundamental set*[7] $\pi_1(X, \mathcal{C})$. This gives us a natural mapping

1 (4.1) $$\mathbf{P}^1(\mathbb{Q}) \times \mathbf{P}^1(\mathbb{Q}) \quad \xrightarrow{\phi} \quad \pi_1(X, \mathcal{C})$$

  with various properties:

  (i) The range of ϕ in Equation 4.1—i.e., $\pi_1(X, \mathcal{C})$—has a natural partial multiplication law[8] as does the domain where $(a/b, c/d) \cdot (c'/d', e/f)$ is defined only if $c/d = c'/d'$)—and then defined to be $(a/b, e/f)$.

[7] One can also think of this $\pi_1(X, \mathcal{C})$ as a category, the *objects* being the elements of $\mathcal{C}$ and the set of —it morphisms $x \to y$ from one object to another being the set of relative homotopy classes of paths in X from x to y.

[8] —which is just composition of morphisms in the vocabulary of the previous footnote—

(ii) The mapping ϕ is invariant under the action of Γ; i.e., for $\gamma \in \Gamma$,

$$\ll \gamma(a/b), \gamma(c/d) \gg = \ll a/b, c/d \gg .$$

(iii) If $\gamma \in \Gamma$ has a pair of complex conjugate fixed points, then for every $r \in \mathbf{P}^1(\mathbb{Q})$

$$\ll \gamma(r), r \gg \quad = \quad 1 \quad \in \quad \pi_1(X, \bar{u}(r)),$$

i.e., it is the trivial element.

Query: *Is there some literature about this? An easy exercise is that the mapping ϕ is surjective. Do the above three relations generate an equivalence relation rendering the mapping induced from ϕ an isomorphism from (such) equivalence classes in $\mathbf{P}^1(\mathbb{Q}) \times \mathbf{P}^1(\mathbb{Q})$ onto $\pi_1(X, \mathcal{C})$?*

We will be interested in this structure specifically when $X = X_0(N)$ for some level N, noting for the moment that $X = X_0(N)$ has a natural definition as a curve over $\mathbb{R}$ such that the involution $X(\mathbf{C}) \to X(\mathbf{C})$ given by complex conjugation is compatible the involution $z \mapsto -\bar{z}$ in connection with the uniformization $\mathbf{H} \to Y \subset X$.

Now suppose that we have an *optimal uniformization*[9] of an elliptic curve E over $\mathbb{Q}$ by $X_0(N)$, i.e., a mapping defined over $\mathbb{Q}$:

$$\lambda : X = X_0(N) \to E$$

that doesn't factor through another elliptic curve (and sends the cusp ∞ to the origin of E).

This induces a mapping $\pi_1(X(\mathbb{C}); \mathcal{C}) \to \pi_1(E(\mathbb{C}); \mathcal{C}_E)$ where $\mathcal{C}_E$ is the image of the cusps in E. By a theorem of Manin-Drinfeld, $\mathcal{C}_E$ consists of elements of finite order in E.

Exercise: Let δ be the lcm of the orders of rational torsion points of E. There's a natural mapping

$$\pi_1(E(\mathbb{C}); \mathcal{C}_E) \to \frac{1}{\delta} H_1(E(\mathbb{C}), \mathbb{Z}) \subset H_1(E(\mathbb{C}), \mathbb{Q}).$$

(Given this uniformization) there are natural generators

$$\eta^{\pm} \in H_1(E(\mathbb{C}), \mathbb{Z})^{\pm},$$

in the $\pm$ eigenspaces of complex conjugation acting on $H_1(E(\mathbb{C}), \mathbb{Z})$ such that for any element $r \in \mathbb{Q} \sqcup \{\infty\} = \mathbf{P}^1(\mathbb{Q})$ the symmetrized and anti-symmetrized images of $\ll \infty, r \gg$ in $H_1(E(\mathbb{C}), \mathbb{Q})$ can be written

---

[9] **Here are a few comments on the notion of** *optimal uniformization of elliptic curves*:

A very good discussion of the issue is in William Stein's *Optimal Elliptic Curve Quotients* `https://wstein.org/papers/ars-manin/html/node2.html`.

If $u : X_0(N) \to E$ is a uniformization (i.e., a nonconstant map to an elliptic curve E over $\mathbb{Q}$) its "modular degree" is the degree of the map u. If there were a factorization of u

$$X_0(N) \xrightarrow{u'} E' \xrightarrow{v} E$$

with v not an isomorphism, u' would have smaller degree .This can't go on indefinitely. *An* **optimal uniformization** is just one that doesn't factor nontrivially. An equivalent way of thinking of such a thing is to consider the mapping induced from u on the jacobian $J_0(N)$ of the modular curve $X_0(N)$: $u_J : J_0(N) \to E$, noting that the kernel of u_J is a subgroup (scheme) G of $J_0(N)$ and if it were not connected, the quotient $J_0(N)$ by G^o, its identity component, would produce a nontrivial factorization of u. So, u is optimal if and only if u_J is connected. That an optimal uniformization is unique (up to multiplication by ± 1, the only automorphisms of elliptic curves that are defined over $\mathbb{Q}$) follows from the multiplicity one theorem regarding Hecke newforms (this opens up another discussion). There is, of course, also a good deal more to say about uniformizations—the fact that a uniformization orients the connected component of the real locus of E (by considering the image of the tangent vector at the cusp $i\infty$ that points downward in $\mathbf{H}$) and about the connection between unformizations and $\Omega_E^{\pm}$.

as $[r]^\pm \cdot \eta^\pm \in \frac{1}{\delta} H_1(E(\mathbb{C}), \mathbb{Z})^\pm$. Note that

$$[r]^\pm \in \delta^{-1}\mathbb{Z}$$

and these are the **normalized modular symbols** that will be (re)-introduced in a moment..

5. Basic properties of modular symbols

For a neat introduction to modular symbols, with some examples of data, see William Stein's *Introduction to Modular Symbols* referenced above.

Fix once and for all an elliptic curve E defined over $\mathbb{Q}$. We will usually suppress E from the notation. Let N be the conductor of E, and f_E the corresponding newform on $X_0(N)$.

$$f_E(q) = \sum_{n \geq 1} a_n q^n.$$

Definition 5.1. Let $\Omega_E^\pm = \Omega^\pm$ denote the real and imaginary periods of E. For every $r \in \mathbb{Q}$ define the (raw) modular symbols

$$\{r\}_E = \{r\} := 2\pi i \int_{i\infty}^{r} f_E(z) dz \in \mathbb{C}$$

and the plus/minus normalized modular symbols

$$[r]_E^\pm = [r]^\pm := \frac{\{r\} \pm \{-r\}}{2\Omega^\pm}.$$

We make the convention that Ω^+ and $[r]_E^+$ are denoted simply Ω and $[r]$ respectively, when the context makes it clear that that's what they should be.

The modular symbols have the following well-known properties.

manybullets

Lemma 5.2. *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

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

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* $\mathbf{H}$, *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* ℓ *is a prime, and* a_ℓ *is the* ℓ*-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:

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

with $a, b, c, d \in \mathbf{Z}$ 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 $ade \equiv 1 (\mathrm{mod}\ f)$ (the latter because $\det(W_e) = e$).

The proof of (vii) is straightforward. □

modsymb1

6. Modular symbols and L-values

Definition 6.1. Suppose χ is a primitive Dirichlet character of conductor m. Define the Gauss sum

$$\tau(\chi) := \sum_{a=1}^{m} \chi(a) e^{2\pi i a/m}$$

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 $\mathrm{Gal}(F/\mathbb{Q})$ with primitive Dirichlet characters of conductor dividing m in the usual way.

Proposition 6.2. *If $F/\mathbb{Q}$ is a finite abelian extension, then*

$$L(E_{/F}, s) = \prod_{\chi:\mathrm{Gal}(F/\mathbb{Q})\to\mathbb{C}^\times} L(E,\chi,s).$$

Corollary 6.3. *If the Birch and Swinnerton-Dyer conjecture holds for $E_{/\mathbb{Q}}$ and $E_{/F}$, then*

BSwD

$$\mathrm{rank}(E(F)) = \mathrm{rank}(E(\mathbb{Q})) + \sum_{\substack{\chi:\mathrm{Gal}(F/\mathbb{Q})\to\mathbb{C}^\times \\ \chi\neq 1}} \mathrm{ord}_{s=1} L(E,\chi,s). \tag{6.4}$$

BS

Theorem 6.5 (Birch-Stevens)**.** *If χ is a primitive Dirichlet character of conductor m, then*

BSt

$$\sum_{a=1}^{m} \chi(a)[a/m]^\epsilon = \frac{\tau(\chi) L(E,\bar{\chi},1)}{\Omega^\epsilon}. \tag{6.6}$$

where the sign ϵ is equal to the sign of the character χ, i.e., $\epsilon = \chi(-1)$.

Note: If χ is of order $p > 2$, a prime number, so

$$\chi : \mathrm{Gal}(F/\mathbb{Q} \to \mu_p := \{e^{(2\pi i j)/p};\ j = 0, 1, \ldots, p-1\} \subset \mathbb{C}^*,$$

and if χ' is any *Galois conjugate character* to χ—equivalently: $\chi' = \chi^a$, for some exponent a not congruent to 0 mod p— then the following are equivalent:

(i) $L(E,\bar{\chi},1)=0$.
(ii) $L(E,\bar{\chi}',1)=0$.
(iii) The value of $[a/m]$ is independent of the numerator a.
(iv) *(conditional on BSD:)* $\operatorname{rank}(E(F)) \geq \operatorname{rank}(E(\mathbb{Q})) + p - 1$.

7. θ-elements and θ-coefficients

Definition 7.1. Suppose $m \geq 1$, and let $G_m = \operatorname{Gal}(\mathbb{Q}(\boldsymbol{\mu}_m)/\mathbb{Q})$. 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 $\boldsymbol{\mu}_m$ as raising to the a-th power). Define

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

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

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

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

$$\mathbb{Z}[\operatorname{Gal}(\mathbb{Q}(\boldsymbol{\mu}_m)/\mathbb{Q})] \to \mathbb{Z}[\operatorname{Gal}(F/\mathbb{Q})].$$

By Lemma 5.2(i) we have

intval (7.2) $$\theta_F^\pm = \sum_{\gamma\in\operatorname{Gal}(F/\mathbb{Q})} c_{F,\gamma}^\pm \cdot \gamma \in \mathbb{Z}[\operatorname{Gal}(F/\mathbb{Q})]$$

where

$$c_{F,\gamma}^\pm = \delta \sum_{\substack{a \pmod m \\ \sigma_{a,m}|_F=\gamma}} [a/m]^\pm.$$

We will refer to the $c_{F,\gamma}^\pm \in \mathbb{Z}$ as *θ-coefficients*. Since we will most often be dealing with the 'plus'-θ-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

tc (7.3) $$c_{F,\gamma} = 2\delta \cdot \sum_{\substack{a\in(\mathbb{Z}/m\mathbb{Z})^\times/\{\pm1\} \\ \sigma_{a,m}|_F=\gamma}} [a/m].$$

With this notation, Proposition 6.5 can be rephrased as follows:

thetaL **Corollary 7.4.** *Suppose $F/\mathbb{Q}$ is a finite real cyclic extension of conductor m and $\chi : (\mathbb{Z}/m\mathbb{Z})^\times \twoheadrightarrow \mathrm{Gal}(F/\mathbb{Q}) \hookrightarrow \mathbb{C}^\times$ is a character that cuts out F. Then*

$$\bar{\chi}(\theta_F) = \delta \frac{\tau(\bar{\chi}) L(E, \chi, 1)}{\Omega}.$$

A natural project: Give a corresponding formulation of θ-elements for abelian varieties over any number field.