Learning seminar on Euler systems: Introduction (Talk 1)

Arshay Sheth

In this talk, we briefly explain what Euler systems are and why they are useful in number theory. We also give an introduction to the three classical examples of Euler systems that we will study in this seminar: cyclotomic units, elliptic units and Heegner points.

§1 Motivation: special values of L-functions

The study of special values of L-functions and their deep connections with various objects of arithmetic interest is an ancient theme in number theory. For example, the formulas

$$\frac{1}{1} - \frac{1}{3} + \frac{1}{5} - \frac{1}{7} + \frac{1}{9} - \frac{1}{11} + \frac{1}{13} - \cdots = \frac{\pi}{4}$$

(Madhava, 14th century & Gregory–Leibniz, 17th century)

$$\frac{1}{1} - \frac{1}{3} - \frac{1}{5} + \frac{1}{7} + \frac{1}{9} - \frac{1}{11} - \frac{1}{13} + \cdots = \frac{\log(1+\sqrt{2})}{\sqrt{2}}$$

(Dirichlet, 1837)

encode, respectively, the following facts:

- The ring of Gaussian integers $\mathbb{Z}[i]$ is a unique factorization domain.
- $(1, 1)$ is a fundamental solution to the Pell equation $x^2 - 2y^2 = -1$.

Indeed, both these formulas are special cases of *the class number formula* for quadratic fields. Let F be a quadratic number field; we can write $F = \mathbb{Q}(\sqrt{m})$ for some square-free $m \in \mathbb{Z}$. It is a standard fact from algebraic number theory that $F \subseteq \mathbb{Q}(\zeta_{D_F})$, where ζ_{D_F} is a primitive D_F-th root of unity and

$$D_F = \begin{cases} 4|m| & \text{if } m \equiv 2, 3 \bmod 4 \\ |m| & \text{if } m \equiv 1 \bmod 4. \end{cases}$$

is the absolute value of the discrminant of F.

We let χ_F denote the Dirichlet character

$$\chi_F : (\mathbb{Z}/d\mathbb{Z})^\times \cong \mathrm{Gal}(\mathbb{Q}(\zeta_d)/\mathbb{Q}) \twoheadrightarrow \mathrm{Gal}(F/\mathbb{Q}) \cong \{\pm 1\} \subseteq \mathbb{C}^\times.$$

The character χ_F has an explicit description in terms of Legendre symbols: for instance, when p is an odd prime then $\chi_F(p) = \left(\frac{m}{p}\right)$.

Let

$$L(\chi_F, s) = \sum_{n=1}^{\infty} \frac{\chi_F(n)}{n^s}$$

be the Dirichlet L-function associated to χ_F.

Theorem 1.1 (Class number formula for imaginary quadratic fields)
If F is an imaginary quadratic field, we have that

$$L(\chi_F, 1) = \frac{2\pi}{w_F\sqrt{D_F}} \cdot h_F,$$

where w_F is the number of roots of unity in F and h_F is the class number of F .

The Madhava–Gregory–Leibniz formula follows by letting $F = \mathbb{Q}(i)$ and noting that $\chi_F : (\mathbb{Z}/4\mathbb{Z})^\times \to \{\pm 1\}$ is the character defined by $\chi(1) = 1$ and $\chi(3) = -1$.

Theorem 1.2 (Class number formula for real quadratic fields)
If F is a real quadratic field, we have that

$$L(\chi_F, 1) = \frac{2}{w_F\sqrt{D_F}} \cdot h_F \cdot \log(\epsilon_F),$$

where w_F is the number of roots of unity in F, h_F is the class number of F and ϵ_F is the fundamental unit of F.

Dirichlet's formula follows by letting $F = \mathbb{Q}(\sqrt{2})$ and noting that $\chi_F : (\mathbb{Z}/8\mathbb{Z})^\times \to \{\pm 1\}$ is the character defined by $\chi(1) = 1, \chi(3) = -1, \chi(5) = -1, \chi(7) = 1$.

The class number formula can be generalised to any number field:

Theorem 1.3 (The analytic class number formula)
Let F be a number field, ζ_F its Dedekind zeta function, h_F its class number, D_F its discriminant, R_F the regulator, w_F the number of roots of unity in F, r_1 the number of real places and r_2 the number of complex places of K. Then:

$$\lim_{s\to 1}(s-1)\zeta_F(s) = \frac{2^{r_1}(2\pi)^{r_2}h_F R_F}{w_F\sqrt{|D_F|}}$$

To recover the class number formula for quadratic fields, we note that $\zeta_F(s) = L(\chi_F, s)\zeta(s)$ and so $\lim_{s\to 1}(s-1)\zeta_F(s) = L(\chi_F, 1)$. Using the functional equation of the Dedekind zeta function, there is an equivalent way of phrasing the analytic class number formula:

Theorem 1.4 (Equivalent version of the analytic class number formula)
Let F be a number field. Then

$$\text{ord}_{s=0}\zeta_F(s) = \text{rank}(\mathcal{O}_F^\times) = r_1 + r_2 - 1$$

and the leading term of $\zeta_F(s)$ at $s = 0$ is $\frac{-h_F \cdot R_F}{w_F}$.

The analog of the class number formula for elliptic curves is the celebrated Birch and Swinnerton-Dyer conjecture, which bears a striking resembalance to the equivalent version of the analytic class number formula.

Conjecture 1.5 (The Birch and Swinnerton-Dyer conjecture)
If $E/\mathbb{Q}$ is an elliptic curve, $L(E,s)$ is its L-function and r_E is the rank of the finitely generated group $E(\mathbb{Q})$, then

$$\operatorname{ord}_{s=1} L(E,s) = r_E.$$

Moreover, the leading term in the Taylor coefficient of $L(E,s)$ at $s=1$ is given by

$$\frac{\#Ш(E)\Omega_E R_E \prod_{p|N} c_p}{(\#E(\mathbb{Q})_{\mathrm{Tor}})^2},$$

where $Ш(E)$ is the Tate–Shafarevich group of E, R_E is the regulator of E, c_p is the Tamagawa number at a prime p dividing the conductor N of E, ω_E is the real period of E multiplied by the number of connected componenets of E and $E(\mathbb{Q})_{\mathrm{Tor}}$ denotes the torsion subgroup of $E(\mathbb{Q})$.

As the above examples show, there are deep relations

$$\boxed{L\text{-functions}} \leftrightarrow \boxed{\text{Arithmetic objects}}.$$

One way to provide a bridge between these two sides is via the the theory of Euler systems. Since the actual definition of an Euler system is rather technical, we explain the rough idea of what an Euler system is rather than giving the precise definition: an Euler system is a coherent collection of objects that can be regarded as an "arithmetic incarnation" or an "arithmetic shape" of L-functions. The objects we have in mind here are things such as units in rings of integers of number fields, points on elliptic curves or cycles on algebraic varieties. The following is a key feature of Euler systems, which make them useful in proving certain cases of various conjectures on special values of L-functions:

Euler systems enable us to give upper bounds for the order of various arithmetic objects such as ideal class groups, Tate–Shafarevich groups and more general Selmer groups.

We briefly explain this in the next section via a simple example.

§2 An example

Let $F = \mathbb{Q}(\sqrt{D})$ be a real quadratic field with discriminant D. By Dirichlet's class number formula for real quadratic fields (Theorem 1.2)

$$L(\chi_F, 1) = \frac{2}{\sqrt{D}} h_F \cdot \log(\epsilon_F).$$

On the other hand, we also have another classical formula for $L(\chi_F, 1)$:

$$L(\chi_F, 1) = \frac{-\tau(\chi_F)}{D} \sum_{a \in \mathbb{Z}/D\mathbb{Z})^\times} \chi_F(a)^{-1} \log|1 - \zeta_D^a|,$$

where $\tau(\chi_F) := \sum_{a \in (\mathbb{Z}/D\mathbb{Z})^\times} \chi_F(a)\zeta_D^a$ is the Gauss sum attached to χ_F. It is a standard fact that $|\tau(\chi_F)| = \sqrt{D}$.

We let

$$u_F := \prod_{a \in (\mathbb{Z}/D\mathbb{Z})^\times} (1 - \zeta_D^a)^{-\chi_D(a)}$$

and it is a fact that $u_F \in \mathcal{O}_F^\times$. By taking absolute values on the two expressions for $L(\chi_D, 1)$, we see that

$$\frac{1}{\sqrt{D}} 2h_F \log(\epsilon_F). = \frac{1}{\sqrt{D}} \log u_F.$$

Thus,

$$\epsilon_F^{2h_F} = u_F$$

and

$$2h_F = [\mathcal{O}_F^\times / \{\pm 1\} : \langle u_F \rangle]$$

The element u_F is an example of a cyclotomic unit (we refer to the next section for the definition) and cyclotomic units are one of the first examples of Euler systems. Thus, the previous formula gives us a relation

Index of an element of an Euler System in a certain group $\leftrightarrow$ **Size of a (generalized) class group**

We label this relation as $(*)$ and we will see that it will appear in each of the three examples of Euler systems we discuss in this learning seminar. The main theme of this learning seminar is to understand how equations like $(*)$ are proved and why they help us make progress on conjectures about special values of L-functions.

§3 Cyclotomic units

We consider the number field $\mathbb{Q}(\zeta_m)$ and let V_m be the subgroup of $\mathbb{Q}(\zeta_m)^\times$ generated by $\pm\zeta_m$ and $1 - \zeta_m^a$ for $1 \leq a \leq m-1$.

Definition 3.1 (Cyclotomic units in $\mathbb{Q}(\zeta_m)$)**.** The group of cyclotomic units in $\mathbb{Q}(\zeta_m)$ is defined to be $C_m := \mathbb{Z}[\zeta_m]^\times \cap V_m$.

Definition 3.2. Let $F/\mathbb{Q}$ be an abelian extension. Let m be the minimal natural number such that $F \subseteq \mathbb{Q}(\zeta_m)$ (such an m exists by the Kronecker–Weber theorem). We define the group of cylcotomic units of F to be $C_m \cap \mathcal{O}_F^\times$.

As indicated in our rough outline of what Euler systems are, we would like the cyclotomic units to form a "coherent" or compatible collection. This is indeed the case: if ℓ is a prime, and if we let $N : \mathbb{Q}(\zeta_{m\ell}) \to \mathbb{Q}(\zeta_m)$ denote the norm map, then we have:

Proposition 3.3 (Norm relations for cyclotomic units)
We have that

$$N(1 - \zeta_{m\ell}) = \begin{cases} 1 - \zeta_m & \text{if } \ell | m \\ (1 - \zeta_m)^{1 - \sigma_\ell^{-1}} = \frac{1 - \zeta_m}{1 - \sigma_\ell^{-1}(\zeta_m)} & \text{if } \ell \nmid m \end{cases}$$

where $\sigma_\ell \in \mathrm{Gal}(\mathbb{Q}(\zeta_m)/\mathbb{Q})$ is the Frobenius element above ℓ.

let p be an odd prime, let $\mathbb{Q}(\zeta_p)^+ := \mathbb{Q}(\zeta_p + \zeta_p^{-1})$, let $\mathbb{Z}[\zeta_p]^+$ denote its ring of integers, and let C_m^+ be the group of cylcotomic units of $\mathbb{Q}(\zeta_p)^+$. As an example of the relation $(*)$, we have the following result:

Theorem 3.4

We have that $[\mathbb{Z}[\zeta_p]^+ : C_m^+]$ is equal to the class number of $\mathbb{Q}(\zeta_p)^+$.

Cyclotomic units have further applications: in the next talk, we will see how they can be used to prove one inclusion of the Iwasawa main conjecture.

§4 Example 2: Elliptic units

Let K be an imaginary quadratic field with class number one. Let E be an elliptic curve with complex multiplication by $\mathcal{O}_K$. It is fact that that we can attach to E a Hecke character

$$\psi : \mathbb{A}_K^\times \to \mathbb{C}^\times$$

satisfying certain properties. Let $\mathfrak{f} \subseteq \mathcal{O}_K$ be the conductor of ψ. Let $\mathfrak{a}$ be an ideal of $\mathcal{O}_K$ coprime to 6 $\mathfrak{f}$.

Definition 4.1. Choose a Weirestass equation for E and let $\Delta(E)$ denote its discriminant. Let $\gamma \in \mathcal{O}_K$ be a generator of $\mathfrak{a}$ and define

$$\theta_{E,\mathfrak{a}} := \gamma^{-12} \cdot \Delta(E)^{N(\mathfrak{a})-1} \cdot \prod_{P \in E\mathfrak{a}} (x - x(P))^{-6} \in K(x).$$

Evaluating this rational function at certain torsion points of elliptic curves gives us units in abelian extensions of K:

Theorem 4.2

Let $\mathfrak{b}$ be a non-trivial ideal of $\mathcal{O}_K$ coprime to $\mathfrak{a}$. Let $Q \in E[\mathfrak{b}]$ be an element of exact order $\mathfrak{b}$. If $\mathfrak{b}$ is not a power of a prime ideal,

$$\theta_{E,\mathfrak{a}}(Q) \in \mathcal{O}_{K(\mathfrak{b})},$$

where $K(\mathfrak{b})$ is the ray class field of K with respect to the ideal $\mathfrak{b}$.

Definition 4.3. Let $S \in E$ be an $\mathcal{O}$-generator of $E[\mathfrak{f}]$. Define

$$\Lambda_{E,\mathfrak{a}} = \prod_{\sigma \in \mathrm{Gal}(K(\mathfrak{f})/K)} \theta_{E,\mathfrak{a}} \circ \tau_{S^\sigma} \in K(x),$$

where $\tau_{S^\sigma}(P) = P + S^\sigma$.

Choose a prime ideal $\mathfrak{p}$ of K coprime to 6 $\mathfrak{f}\mathfrak{a}$ and let $\mathcal{R}$ be the collection of squarefree integral ideals of $\mathcal{O}_K$ coprime to $6\mathfrak{a}\mathfrak{f}\mathfrak{p}$. Let $K_n = K(E[\mathfrak{p}^n])$ and given $\mathfrak{r} \in \mathcal{R}$, we let $K_n(\mathfrak{r}) = K_n(E[\mathfrak{r}])$. We fix an isomorphism $\xi : \mathbb{C}/L \to E(\mathbb{C})$, where L is a lattice which we can write as $\Omega \cdot \mathcal{O}_K$ for some $\Omega \in \mathbb{C}$.

Definition 4.4 (Elliptic units)**.** For all $n \in \mathbb{N}$ and $\mathfrak{r} \in \mathcal{R}$, we define the elliptic units of K to be

$$\eta_n(\mathfrak{r}) = \Lambda_{E,\mathfrak{a}}(\xi(\psi(\mathfrak{p}^n\mathfrak{r})^{-1}\Omega)) \in \mathcal{O}_{K_n(\mathfrak{r})^\times}.$$

Elliptic units form an Euler system; indeed they satisfy the two key features of Euler systems that we mentioned in the first section.

- They satisfy compatibility relations for varying n and $\mathfrak{r}$. For example, the following norm relation is completely analogous to those satisfied by cyclotomic units: let $\mathfrak{b}' = \mathfrak{b}\mathfrak{p}^{-1}$ and $\mathfrak{p} = (\pi)$. Then we have that

$$N_{K(\mathfrak{b}')/K(\mathfrak{b})}\theta_{E,\mathfrak{a}}(Q) = \begin{cases} \theta_{E,\mathfrak{a}}(\pi Q) & \text{if } \mathfrak{p} | \mathfrak{b}' \\ \theta_{E,\mathfrak{a}}(\pi Q)^{1-\sigma_{\mathfrak{p}}^{-1}} & \text{if } \mathfrak{p} \nmid \mathfrak{b}' \end{cases}$$

  where $\sigma_{\mathfrak{p}} \in \mathrm{Gal}(K(\mathfrak{b})/K)$ is the Frobenius element above $\mathfrak{p}$.

- They are related to L-functions. Firstly, it is an important result that since E has CM by K with associated Hecke character ψ, the L-function of E is essentially a Hecke L-function: we have that $L(E/K, s) = L_{\mathfrak{f}}(\psi, s) \cdot L_{\mathfrak{f}}(\overline{\psi}, s)$. The relation between elliptic units and L-functions is then provided by the following formula, which is sometimes called the "Kronecker limit formula"

Theorem 4.5

We have that

$$\frac{d}{dz^k} \log \Lambda_{E,a}(z) = 12(-1)^k (k-1)! f^k (N(\mathfrak{a}) - \psi(a)^k) \Omega^{-k} L_{\mathfrak{f}}(\overline{\psi}^k, k),$$

where $\mathfrak{f} = (f)$.

We now briefly indicate how the Euler system of elliptic units can be used to prove a relation such as (*). To do so, we first set up a bit of notation. Let $F = K(E(\mathfrak{p}])$, $\Delta = \mathrm{Gal}(F/K)$, and A be the ideal class group of F. Let $\chi : \Delta \to \mathbb{Z}_p^\times$ be a character. If M is a finitely generated Δ-module, and hence a $\mathbb{Z}[\Delta]$-module, $M^{(p)} := M \otimes_{\mathbb{Z}} \mathbb{Z}_p$ is a $\mathbb{Z}_p$-module. We let

$$M^\chi = \{m \in M^{(p)} : \sigma \cdot m = \chi(\sigma) \cdot m \quad \forall \sigma \in \Delta\}.$$

Theorem 4.6 (An example of $(*)$)

Let C be the $\mathbb{Z}[\Delta]$-submodule of $\mathcal{O}_F^\times$ generated by μ_F and $\eta_1(\mathcal{O}_K)$. Then

$$\#A^\chi \leq \#(\mathcal{O}_F^\times / C)^\chi.$$

As an application, we will see how this theorem was used to prove one of the first results on the Birch and Swinnerton–Dyer conjecture:

Theorem 4.7 (Coates–Wiles)

Suppose E is a CM elliptic curve defined over $\mathbb{Q}$. If $L(E, 1) \neq 0$, then $E(\mathbb{Q})$ is finite.

As a summary of the previous two sections, we provide a list of analogies between cylcotomic units and elliptic units:

Cyclotomic Units	Elliptic Units
Units in cyclotomic fields (ray class field for $\mathbb{Q}$)	Units in ray class fields of K
Provide bounds on class groups of cyclotomic fields	Provide bounds on class groups of ray class fields
Related to Dirichlet L-functions	Related to L-functions of elliptic curves

§5 Example 3: Heegner Points

Let $E/\mathbb{Q}$ be an elliptic curve with conductor N. Let $Y_0(N)$ denote the modular curve corresponding to the congruence subgroup $\Gamma_0(N)$. $Y_0(N)$ is an algebraic curve defined over $\mathbb{Q}$ and has the following moduli interpretation: we have that $Y_0(N)(\mathbb{C})$ is in bijection with

$$\{\phi : E \to E' | E, E' \text{ e.c. over } \mathbb{C} \ \& \ \ker(\phi) \text{ cyclic subgroup of order } N\}/\cong$$

If K is a number field, then $Y_0(N)(K)$ is in bijection with

$$\{\phi : E \to E' | E, E' \text{ e.c. over } K, \ \ \phi \text{ defined over } K \& \ \ker(\phi) \text{ cyclic subgroup of order } N\}/\cong,$$

where the "$\cong$" means over $\overline{K}$.

Definition 5.1 (Heegner points on modular curves)**.** We say that $x_K = (\phi : E \to E') \in Y_0(N)(\mathbb{C})$ is a Heegner point, if both E and E' have complex multiplication by some order $\mathcal{O} \subseteq K$.

Fix an imaginary quadratic field K with discriminant D satisfying the following "Heegner hypothesis:": every prime p dividing N splits completely in K (one can show that there are infinitely many quadratic fields satisfying this condition). Let $\mathcal{N}$ be an ideal such that $\mathcal{O}_K/\mathcal{N} \cong \mathbb{Z}/N\mathbb{Z}$ (such an ideal exists for imaginary quadratic fields satisfying the Heegner hypothesis). Every order $\mathcal{O}$ is of the form $\mathcal{O} = \mathbb{Z} + n\mathcal{O}_K$ for some $n \geq 1$. Here n is called the conductor of $\mathcal{O}$ and we denote $\mathcal{O}$ by $\mathcal{O}_n$. Let $\mathcal{N}_n := \mathcal{N} \cap \mathcal{O}_n$. For each n relatively prime to DN, one can check that $\mathcal{O}_n/\mathcal{N}_n \cong \mathbb{Z}/N\mathbb{Z}$.

Definition 5.2. For each n relatively prime to ND, the Heegner point of conductor n is defined to be

$$x_n := [\mathbb{C}/\mathcal{O}_n \to \mathbb{C}/\mathcal{N}_n^{-1}] \in Y_0(N)(\mathbb{C}).$$

Using CM theory, one can show that x_n actually lies in $Y_0(N)(H_n)$, where H_n is the ring class field of $\mathcal{O}_n$. To define Heegner points over elliptic curves, we first recall

Theorem 5.3 (Shimura-Taniyama conjecture/Modularity theorem)
Let E be an elliptic curve defined over $\mathbb{Q}$ with conductor N. Then there exists a non-zero morphism

$$\varphi : X_0(N) \to E.$$

defined over $\mathbb{Q}$.

Definition 5.4 (Heegner points on elliptic curves)**.** Let E be as above and let K be an imaginary quadratic field satisfying the Heegner hypothesis. Fix a modular parameterization φ as above. The Heegner point of conductor n is defined to be

$$y_n := \varphi(x_n) \in E(H_n).$$

Definition 5.5 (The basic Heegner point)**.** We define

$$y_K := \mathrm{tr}_{H_1/K}(y_1) = \sum_{\sigma \in \mathrm{Gal}(H_1/K)} \sigma(y_1) \in E(K)$$

and call it the Basic Heegner point.

The set of Heegner points form an Euler system; they are compatible under trace maps and are related to L-functions via the Gross-Zagier formula. We briefly explain each of these two aspects.

We define

$$\mathrm{Tr}_n : E(H_{np}) \to E(H_n), \quad z \mapsto \sum_{\sigma \in \mathrm{Gal}(H_{np}/H_n)} \sigma(z)$$

Theorem 5.6

We have that $\mathrm{Tr}(y_{np}) = a_p y_n$, where $a_p = p + 1 - \#E(\mathbb{F}_p)$.

Theorem 5.7 (The Gross-Zagier formula)

Let E be an elliptic curve over $\mathbb{Q}$ and let K be an imaginary quadratic field which satisfies the Heegner hypothesis. Let E_K denote the elliptic curve E over K.

Then we have

$$L'(E_K, 1) = c_{E,K} \cdot \langle y_K, y_K \rangle$$

where $c_{E,K} \in \mathbb{C}$ is some constant depending on E and K and $\langle , \rangle$ is the Neron–Tate height pairing.

We denote by $r_{\mathrm{an}}(E_K)$ the order of vanishing of the L-function of E_K and by $r_{\mathrm{al}}(E_K)$. Using the fact that $\langle P, P \rangle = 0$ if and only if P is a torsion point, we deduce:

Corollary 5.8

We have that $r_{\mathrm{an}}(E_K) = 1 \implies r_{\mathrm{al}}(E_K) \geq 1$.

Proof. $r_{\mathrm{an}}(E_K) = 1 \implies L'(E_K, 1) \neq 0 \implies \langle y_K, y_K \rangle \neq 0 \implies y_K$ is a non-torsion point $\implies r_{\mathrm{al}}(E_K) \geq 1$. □

Kolyvagin used the Euler system of Heegner points to prove the following:

Theorem 5.9 (Kolyvagin)

If y_K is not torsion, then $r_{al}(E_K) = 1$ and $Ш(E/K)$ is finite with $\#Ш(E/K)$ dividing $[E(K) : \mathbb{Z}y_K]^2 \cdot t_{E/K}$, for a certain $t_{E/K} \in \mathbb{Z}_{\geq 1}$ divisible by primes in an explicit finite set depending on E.

Thus, Kolyvagin's theorem gives us another relation of the form $(*)$. Moreover, Gross-Zagier+ Kolyvagin give us the following:

Corollary 5.10

We have that

$$r_{\mathrm{an}}(E_K) = 1 \implies r_{\mathrm{al}}(E_K) = 1.$$

Using the theory of "descent", this in-turn implies that:

$$r_{\mathrm{an}}(E) = 1 \implies r_{\mathrm{al}}(E) = 1.$$

In the third part of our seminar, we will study the proof of Kolyvagin's theorem.