COMPLEX MULTIPLICATION

COURSE: EUGENIA ROSU AND JAN VONK
NOTES: ROSS PATERSON

Disclaimer. These notes were taken live during lectures at the Spring School on Arithmetic Statistics held at CIRM from 8^{th}–12^{th} May 2023. Any mistakes are the fault of the transcriber and not of the lecturer, they have not been proofread in any meaningful way.

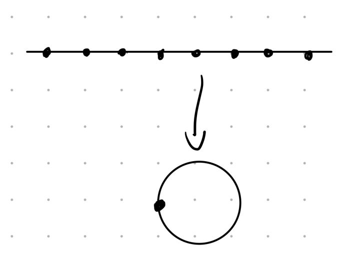
In general, $\sum'$ means take the sum excluding the obvious elements which are not defined (typically 0's)

Lecture 1 (Jan Vonk)

We begin, very classically, with a viewpoint due to Eisenstein. Forget everything you know about trigonometric functions!

1. Cyclotomy

Consider $\mathbb{Z} \subseteq \mathbb{R}$, and think about the quotient $\mathbb{R}/\mathbb{Z}$ which we usually think of as the circle group. We'd like to think of this quotient algebraically.



To do this we shall look at the invariant functions for $k \geq 2$

$$\alpha_k(z) = \sum_{\lambda \in \mathbb{Z}} \frac{1}{(z-\lambda)^k}.$$

Many polynomial relations exist between these (for example $\alpha_2^2 = \alpha_4 + \Omega_2\alpha_2$) with coeficients equal to combinations of

$$\Omega_k := \sum_{\lambda \in \mathbb{Z}'} \frac{1}{\lambda^k}.$$

There are extra terms to add:

- Consider the case $k = 1$, and define in pretty much the same way

$$\alpha_1(z) := \frac{1}{z} + \sum_{\lambda \in \mathbb{Z}'} \frac{1}{z-\lambda} + \frac{1}{\lambda}.$$

This is absolutely convergent (unlike what we would have had if we hadn't modified for $k = 1$) and is translation invariant. It satisfies the relation

$$\alpha_1^2 = \alpha_2 - 3\Omega_2. \tag{1}$$

- We want a multiplicative lift for

$$\mathrm{d}\log/\mathrm{d}z : f \mapsto f'/f$$

for our function α_1. We take

$$\mathfrak{S}(z) := \pi z \prod_{\lambda \in \mathbb{Z}'} \left(1 - \frac{z}{\lambda}\right) \exp\left(\frac{z}{\lambda}\right),$$

and note that we can prove formally the following two identities:

$$(\mathrm{d}\log/\mathrm{d}z)(\mathfrak{S}) = \mathfrak{S}'(z)/\mathfrak{S}(z) = \alpha_1(z)$$
$$\mathfrak{S}(z+1) = -\mathfrak{S}(z)$$

1.1. **Periods.** Euler realised that

$$\mathfrak{S}(z) = \sin(\pi z),$$

so that

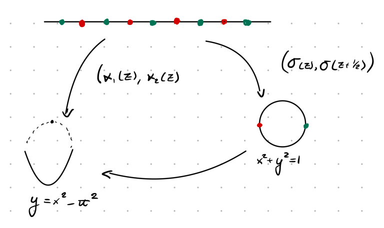
$$\begin{aligned} \alpha_1(z) &= \frac{1}{z} - \sum_{k \geq 2} \Omega_k z^{k-1} \\ &= \pi \cot(\pi z) \\ &= -\pi i (e^{2\pi i z} + 1)/(e^{2\pi i z} - 1). \end{aligned}$$

From this we deduce that for $k \geq 2$

$$\Omega_k = \frac{(2\pi)^k}{k!} |B_k|$$

where B_k are Bernoulli numbers. This leads us nicely on to special values.

1.2. **Special Values.** Consider the set of vaues at division points of $\mathbb{R}/\mathbb{Z}$, i.e. $z \in \mathbb{Q}/\mathbb{Z}$.

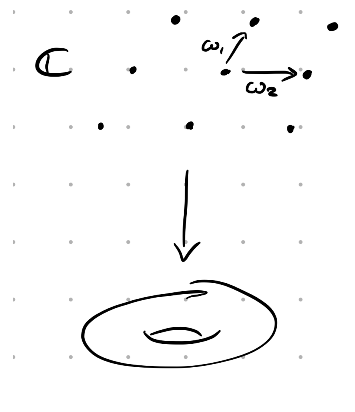


We have the Chebyshev polynomials

$$T_n(\cos(\theta)) = \cos(n\theta),$$

so find that the values of $\sigma(z)$ at division points are algebraic.

Example 1. Consider $z = 2/17$, then we get $\frac{1}{2n}(\zeta_{17} - \zeta_{17}^{-1}) \in \mathbb{Q}(\zeta_{68}) =: K$. It is half of a 17-unit, i.e. it is half of an element in $\mathcal{O}_K[1/17]^\times$.



2. Elliptic Functions

Consider a rank 2 lattice $\Lambda = \mathbb{Z}\omega_1 + \mathbb{Z}\omega_2 \subseteq \mathbb{C}$
Again, we want to find invariant functions. For $k \geq 3$ we define

$$\alpha_k(\Lambda, z) = \sum_{\lambda \in \Lambda} \frac{1}{(z-\lambda)^k}.$$

Outside the range of convergence we define as follows.

- for $k = 2$ we write
$$\alpha_2(\Lambda, z) = \frac{1}{z^2} + \sum_{\lambda \in \Lambda'} \left(\frac{1}{(z-\lambda)^2} - \frac{1}{\lambda^2} \right),$$
which is usually known as the Weierstrass $\wp$-function. This is an invariant function.
- For $k = 1$ we define
$$\alpha_2(\Lambda, z) = \frac{1}{z} + \sum_{\lambda \in \Lambda'} \left(\frac{1}{(z-\lambda)} + \frac{1}{\lambda} + \frac{z}{\lambda^2} \right).$$

This is often called the Weierstrass ζ-function, but it is **NOT** invariant!

We have a transformation law:

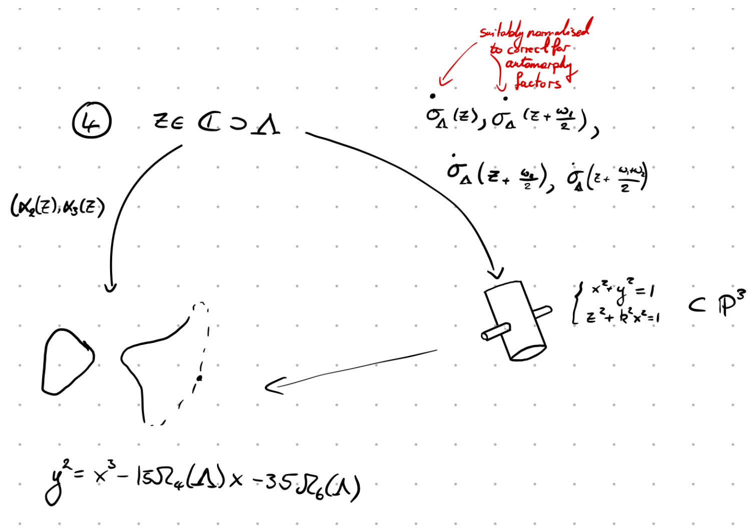
$$\alpha_1(\Lambda, z + \omega_i) = \alpha_1(\Lambda, z) + \eta_i.$$

We have multiplicative lifts given by

$$\sigma(\Lambda, z) := z \prod_{\lambda \in \Lambda'} \left(1 - \frac{z}{\lambda}\right) \exp\left(\frac{z}{\lambda} + \frac{z^2}{2\lambda^2}\right),$$

and it satisfies

$$(\mathrm{d}\log/\mathrm{d}z)(\sigma) = \sigma'(z)/\sigma(z) = \alpha_1(\Lambda, z)$$
$$\sigma(\Lambda, z + \omega_i) = -\exp\left(\eta_i\left(z + \frac{\omega_i}{2}\right)\right)\sigma(\Lambda, z)$$



2.1. **Special Values.** The Values at division points of $\mathbb{C}/\Lambda$

We will study values at division points when Λ has complex multiplication, i.e.

$$\{\alpha \in \mathbb{C} \;:\; \alpha\Lambda \subseteq \Lambda\} \supsetneq \mathbb{Z}.$$

We will look at:

(1) singular moduli, e.g. the j-invariant $j(\Lambda) = \frac{(60\Omega_4(\Lambda))^3}{(60\Omega_4(\Lambda))^3-(140\Omega_6(\Lambda))62}$;

(2) elliptic units, i.e. quotients of σ-functions (Klein forms), for example

$$(\Delta|\gamma)/\Delta$$

for $\gamma \in M_2(\mathbb{Z})$ and Δ the usual Ramanujan modular form.

Some remarks on CM theory:

- Heegner (1952) used CM theory to construct integral points on modular curves $X_{\mathrm{ns}}(p)$, solving the class number 1 problem for imaginary quadratic fields.
- Coates–Wiles (1976) used elliptic units to prove the Birch–Swinnerton-Dyer conjecture in the analytic rank 0 case.
- Gross–Zagier (1985) determine factorisation of (differences of) singular moduli to obtain the Birch–Swinnerton-Dyer conjecture in the analytic rank 1 case.

Lecture 2 (Vonk)

Today: Special values at CM lattices $\Lambda = \alpha\,\langle 1, \tau\rangle$ of

$$\begin{aligned} j(q) :&= \frac{\left(1 + 240\sum_{g\geq 1}\frac{n^3q^n}{1-q^n}\right)}{q\prod_{n\geq 1}(1-q^n)^{24}} \\ &= \frac{1}{q} + 744 + 196884q + 21493760q^2 + \cdots \in q^{-1}\mathbb{Z}[[q]], \end{aligned}$$

as well as of $(\Delta|_\gamma)/\Delta$ for $\gamma \in M_2(\mathbb{Z})$ with $\det(\gamma) = p$.

Notation 2. Pick coset representatives for

$$\mathrm{SL}_2(\mathbb{Z})\backslash\{\gamma \in M_2(\mathbb{Z}) \;:\; \det(\gamma) = p\} =: M_p,$$

by setting (for $j \in \{0, \dots, p-1\}$)

$$\gamma_j := \begin{pmatrix} 1 & j \\ 0 & p \end{pmatrix}$$

$$\gamma_\infty := \begin{pmatrix} p & 0 \\ 0 & 1 \end{pmatrix}$$

3. Singular Moduli

Theorem 3. *There exist $\Phi_p(x,y) \in \mathbb{Z}[x,y]$ such that*

$$\Phi_p(x, j(\tau)) = \prod_{\gamma \in M_p} (x - j(\gamma\tau)) = \mathcal{P}(x).$$

It satisfies $\Phi_p(x,y) = \Phi_p(y,x)$, and the leading coefficient $\Phi_p(x,y) = \pm 1$.

Proof. Coefficients a_i of $\mathcal{P}(x)$ are:

- holomorphic on $\mathfrak{h} = \{z \in \mathbb{C} \;:\; \Im(z) > 0\}$; and
- $\mathrm{SL}_2(\mathbb{Z})$-invariant; and
- meromorphic.

In particular they are in $\mathbb{C}[j]$. Note that $\exp\left(2\pi i \left(\frac{\tau+j}{p}\right)\right) = \zeta_p^j q^{1/p}$ so as q-series in $q^{-1}\mathbb{Z}[\zeta_p][[q]]$ the coefficients are invariant under $\mathrm{Gal}(\mathbb{Q}(\zeta_p)/\mathbb{Q})$. Thus they are in $\mathbb{Z}[j]$.

Th leading term of $j(\tau) - j(\gamma\tau)$ is a root of unity. Thus the leading term of $\Phi_p(x,x)$ must be an integer root of unity, meaning that it must be ± 1. □

Example 4 (Very Large)**.** See the webpage of Drew Sutherland for many excellent huge examples. Here is a small-ish one.

$$\Phi_2(x,x) = (x - 8000)(x + 3375)^2(x - 1728)$$
$$\Phi_3(x,x) = x(x - 2^6 5^3)(x + 2^{15})^2(x - 2^4 3^3 5^3)$$
$$\Phi_5(x,x) = (x^2 - 2^7 5^3 79x - 2^{12} 5^3 11^3)(\text{degree 8 factor})$$

Let $\mathcal{O}$ be an imaginary quadratic order, $\mathfrak{a} \leq \mathcal{O}$ a proper ideal, and p be a prime number such that $p\mathcal{O} = \mathfrak{p}\overline{\mathfrak{p}}$ with $\mathfrak{p}$ principal (this is a positive density choice by Chebotarev). Then

$$\mathfrak{p}\mathfrak{a} \subset \mathfrak{a}$$

is of index $\mathfrak{p}$ and $j(\mathfrak{p}\mathfrak{a}) = j(\mathfrak{a})$ so $j(\mathfrak{a})$ is a root of $\Phi_p(x,x)$, so is an algebraic integer.

Example 5.

$$j(\sqrt{-1}) = 1728$$
$$j(\sqrt{-2}) = 8000$$
$$j\left(\frac{1+\sqrt{-7}}{2}\right) = -3375$$

Moreover $j(\sqrt{-5})$ is a root of $\Phi_5(x)$. Here is a riddle: $j\left(\frac{1+\sqrt{-63}}{2}\right) = -2^{18}3^35^323^329^3 \in \mathbb{Z}$, which polynomial should give this? The answer is 41, try to see this.

Theorem 6 (Kronecker's congruence)**.**

$$\Phi_p(x,y) \equiv (x^p - y)(x - y^p) \mod p$$

Proof. Note that $\exp\left(2\pi i \frac{\tau+j}{p}\right) = \zeta_p^j q^{1/p} \equiv q^{1/p} \mod \zeta_p - 1$, so that

$$\begin{aligned} \Phi_p(x,j) &\equiv (x - j(q^{1/p}))^p (x - j(q^p)) \mod (\zeta_p - 1) \\ &\equiv (x^p - j(q))(x - j(q)^p) \end{aligned}$$

□

For any $p\mathcal{O} = \mathfrak{p}\overline{\mathfrak{p}}$ we have

$$(j(\mathfrak{a})^p - j(\mathfrak{a}\mathfrak{p}))(j(\mathfrak{a}\mathfrak{p})^p - j(\mathfrak{a})) \mod p.$$

Want: We want to prove that this first factor is in fact $\equiv 0 \mod \overline{\mathfrak{p}}$.

4. Some Elliptic Units

Definition 7. For all $\gamma = \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in M_p$, define

$$h_\gamma := (\Delta|\gamma)/\Delta := \det(\gamma)^{12}(c\tau + d)^{-12}\frac{\Delta(\gamma\tau)}{\delta(\tau)}.$$

Theorem 8. *There exists $\Upsilon_p(x,y) \in \mathbb{Z}[x,y]$ such that*

$$\Upsilon(x, j(\tau)) = \prod_{\gamma \in M_p} (x - h_\gamma(\tau)).$$

It satisfies

$$\Upsilon(0,y) = p^{12}$$

Proof. This is in the exercises. □

Example 9. We have

$$\begin{aligned} \Upsilon_2(x,y) &= (x+16)^3 - xy, \\ \Upsilon_3(x,y) &= (x-9)^3(x-729) + 72x(x+21)y - xy^2. \end{aligned}$$

We see that, for $\mathcal{O}$ an imaginary quadratic order and $\mathfrak{a} \subset \mathcal{O}$ a proper ideal, $h_\gamma(\mathfrak{a}) \in \overline{\mathbb{Z}}$. Unfortunately they have no rich prime factorisations, as the next theorem makes precise.

Theorem 10. *Suppose $p\mathcal{O} = \mathfrak{p}\overline{\mathfrak{p}}$ is a proper ideal, then*

$$\left\langle h_{\gamma(\mathfrak{p})}(\mathfrak{a}) \right\rangle = \overline{\mathfrak{p}}^{12}$$

and

$$\left\langle h_{\gamma(\overline{\mathfrak{p}})} \right\rangle (\mathfrak{a}) = \mathfrak{p}^{12},$$

where $\gamma(\mathfrak{p}) \in M_p$ relates the bases of $\mathfrak{a}$ and $\mathfrak{p}\mathfrak{a}$, and $h_\gamma(\mathfrak{a})$ is a unit if $\gamma \neq \gamma(\mathfrak{p})\gamma(\overline{\mathfrak{p}})$

Why is this theorem true? We can make it follow from the previous one.

Proof. Let f be such that $\mathfrak{p}^f = \langle \alpha \rangle$ is principal. Then

$$\left\langle \left(p^{12}\frac{\Delta(\mathfrak{p}^f\mathfrak{a})}{\Delta(\mathfrak{p}^{f-1}\mathfrak{a})}\right)\left(p^{12}\frac{\Delta(\mathfrak{p}^{f-1}\mathfrak{a})}{\Delta(\mathfrak{p}^{f-2}\mathfrak{a})}\right)\cdots\left(p^{12}\frac{\Delta(\mathfrak{p}\mathfrak{a})}{\Delta(\mathfrak{a})}\right)\right\rangle = \langle p^{12f}\alpha^{-12}\rangle = \overline{\mathfrak{p}}^{12f}.$$

Then, writing $\lambda_i = \left(p^{12}\frac{\Delta(\mathfrak{p}^i\mathfrak{a})}{\Delta(\mathfrak{p}^{i-1}\mathfrak{a})}\right)$, we have each $\lambda_i \in \overline{\mathbb{Z}}$ and divides $\overline{\mathfrak{p}}^{12} + \langle p\rangle^{12} = \overline{\mathfrak{p}}^{12}$, and $\langle \lambda_1 \dots \lambda_f\rangle = \overline{\mathfrak{p}}^{12}$. Thus $\langle \lambda_i \rangle = \overline{\mathfrak{p}}^{12}$.

Theorem now follows from

$$h_{\gamma(\mathfrak{p})}(\mathfrak{a})h_{\gamma(\overline{\mathfrak{p}})}(\mathfrak{a})\prod_{\gamma\neq\gamma(\mathfrak{p}),\gamma(\overline{\mathfrak{p}})} h_\gamma(\mathfrak{a}) \equiv \pm p^{12}$$

□

Lecture 3 (Vonk)

Last time we defined two different kinds of algebraic integers:

(1) Singular moduli $j(\mathfrak{a})$, for example

$$j\left(\frac{1+\sqrt{-67}}{2}\right) = -2^{15}3^3 5^3 11^3$$

(2) (some) Elliptic units $h_\gamma(\mathfrak{a})$, where $\gamma \in M_2(\mathbb{Z})$ with $\det(\gamma) = p$ a prime.

Example 11. $h_\gamma(\sqrt{-14}) = \frac{\left(\sqrt{2}+1+\sqrt{2\sqrt{2}-1}\right)^{12}}{2^6}$ for $\gamma = \begin{pmatrix} 1 & 0 \\ 0 & 2\end{pmatrix}$.

Theorem 12. *There exists $\mathcal{G}_p \in \mathbb{Z}[x,y,z]$ such that*

$$\mathcal{G}_p(x,y,j(\tau)) = \sum_{\gamma\in M_p}(x - j(\gamma\tau))\prod_{\delta\neq\gamma}(y-h_\delta).$$

It satisfies

$$\mathcal{G}_p(z^p,y,z) \equiv 0 \mod p$$

Proof. Since $\exp\left(2\pi i\left(\frac{\tau+j}{p}\right)\right) = \zeta_p^j q^{1/p} \cong q^{1/p} \mod \zeta_p - 1$, we find that

$$j(\gamma_0\tau) \equiv j(\gamma_1\tau) \equiv \cdots \equiv j(\gamma_{p-1}\tau) \mod \zeta_p - 1$$

and

$$h_{\gamma_0} \equiv h_{\gamma_1} \equiv \cdots \equiv h_{\gamma_{p-1}} \mod \zeta_p - 1.$$

So it follows that

$$\begin{aligned}\mathcal{G}_p(x,y,j(\tau)) \equiv &\,(x - j(q^p))(y-h_{\gamma_0})^p \\ &+ p\left(x - j(q^{1/p})\right)(y-h_{\gamma_\infty})(y-h_{\gamma_0})^{p-1} \mod \zeta_p - 1\end{aligned}$$

as required. □

Why did we do this? Because it buys us a refinement of Kroneckers congruence!

Theorem 13. *Let $\mathcal{O} \subset K$ be an imaginary quadratic order, $p\mathcal{O} = \mathfrak{p}\overline{\mathfrak{p}}$ proper, $\mathfrak{a} \subset \mathcal{O}$ proper, then*

$$j(\mathfrak{a})^p \cong j(\mathfrak{a}\overline{\mathfrak{p}}) \mod \mathfrak{p}.$$

Proof. Substitute $(x, y, z) = (j(\mathfrak{a})^p, h_{\gamma(\overline{\mathfrak{p}})}(\mathfrak{a}), j(\mathfrak{a}))$ into $\mathcal{G}_p$ above. This gives

$$(j(\mathfrak{a})^p - j(\mathfrak{a}\overline{\mathfrak{p}})) \prod_{\gamma \neq \gamma(\overline{\mathfrak{p}})} (h_{\gamma(\overline{\mathfrak{p}})}(\mathfrak{a}) - h_\gamma(\mathfrak{a})) \equiv 0 \mod \mathfrak{p}$$

However the product is never $0 \mod \mathfrak{p}$, so the leading factor must be $0 \mod \mathfrak{p}$. □

Corollary 14. *Suppose that $\mathfrak{a} \subset \mathcal{O}$ is a proper ideal in an imaginary quadratic order in the quadratic field K. Then $K(j(\mathfrak{a}))$ is the ring class field of $\mathcal{O}$.*

Remark 15. The ring class field of $\mathcal{O}$ is the finite abelian extension $H_{\mathcal{O}}/K$ associated by class field theory to

$$\mathrm{Cl}(\mathcal{O}) \cong \mathbb{C}^\times \tilde{\mathcal{O}}^\times \backslash \mathbb{A}_K^\times / K^\times$$

Proof. We will sketch one direction, and leave the other as an exercise. Let $L = H_{\mathcal{O}}/K$ be the ring class field. Then take any split prime $p\mathcal{O} = \mathfrak{p}\overline{\mathfrak{p}}$ coprime to $\mathrm{disc}(\mathcal{O})$, such that $[\mathcal{O}_M : \mathcal{O}_K[j(\mathfrak{a})]]$ where $M = K(j(\mathfrak{a}))$.

Then p splits completely in $L/\mathbb{Q}$ if and only if $\mathfrak{p}$ is a principal prime of $\mathcal{O}$. In particular, $j(\mathfrak{a}) = j(\mathfrak{p}\mathfrak{a}) \equiv j(\mathfrak{a})^p \mod \overline{\mathfrak{p}}$ and similarly if we swap $\mathfrak{p}$ and $\overline{\mathfrak{p}}$. Thus p splits completely in $K(j(\mathfrak{a})) = M$. It follows from Chebotaryov that $M \subset L$.

Exercise 16. Do the following

(1) Show that also $L \subset M$ using similar ideas, concluding the proof.
(2) Show that $h_\gamma(\mathfrak{a}) \in L$.

□

Specialising to $\mathcal{O} = \mathcal{O}_K$ being maximal, we find the following corollary.

Corollary 17. *Let $\mathfrak{a} \subset \mathcal{O}_K$ be a proper ideal, then $\mathfrak{a}^{12}$ becomes principal in the Hilbert class field H/K.*

Remark 18. This is a weaker in comparison to the principal ideal theorem, but it does give an explicit generator!

Definition 19. The Dedeking eta function is

$$\eta(q) := q^{1/24} \prod_{n \geq 1} (1 - q^n),$$

where, as usual, $q = e^{2\pi i \tau}$.

Remark 20. Note that $\eta^{24}(q) = \Delta(q)$, and it satisfies

$$\eta(\tau + 1) = \zeta_{24}\zeta(\tau)$$
$$\eta(-1/\tau) = \sqrt{-i\tau}\eta(\tau).$$

where for the square root we are choosing the branch that is 1 on the imaginary axis.

The special values at CM points relate to L-functions, by the Kronecker limit formula. This formula is given as follows.

Definition 21. Consider real Eisenstein series

$$E(\tau, s) := \sideset{}{'}\sum_{m,n \in \mathbb{Z}} \frac{\Im(\tau)^s}{|m\tau + n|^{2s}}$$

for $\Re(s) > 1$.

Theorem 22 (Kronecker Limit Formula)**.**

$$E(\tau, s) = \frac{\pi}{s-1} + 2\pi\left(c - \log\left(\sqrt{\Im(\tau)}\,|\eta(\tau)|\right)^2\right) + O(s-1).$$

Specialising to CM points, and using our previous results, we find

$$\zeta_{\mathfrak{a}}(s) = \sum_{\mathfrak{b}\sim\mathfrak{a}} N(\mathfrak{b})^{-s} = \frac{k}{s-1} + c(\mathfrak{a}) + O(s-1),$$

where $c(\mathfrak{a}_1) - c(\mathfrak{a}_2) = \log(u)$ *for* $u \in \mathcal{O}_H^\times$

Lecture 4 (Rosu)

We'll pick up where Jan left off yesterday, and make the jump to the 20th century.

5. Shimura Reciprocity Law

Goal: Shimura reciprocity law.

5.1. **Motivation.** Let $K = \mathbb{Q}(\sqrt{-D})$ for some $D > 0$ be an imaginary quadratic field, let H be the hilber class field of K, let $\mathfrak{a} \leq \mathcal{O}_K$ be an ideal viewed as a lattice in $\mathbb{C}$. To this ideal we have an associated elliptic curve $E_{\mathfrak{a}}$ such that

$$E_{\mathfrak{a}}(\mathbb{C}) \cong \mathbb{C}/\mathfrak{a}.$$

The equation for this curve is given by

$$E_{\mathfrak{a}} : y^2 = 4x^3 - \frac{27j(\mathfrak{a})}{j(\mathfrak{a}) - 1728}x - \frac{27j(\mathfrak{a})}{j(\mathfrak{a}) - 1728}.$$

Moreover, $j(\mathfrak{a}) \in H$.

Theorem 23. *If* $\mathfrak{b} \leq \mathcal{O}_K$ *is an ideal coprime to* $\mathfrak{a}$*, then*

$$j(\mathfrak{a})^{\sigma_{\mathfrak{b}}^{-1}} = j(\mathfrak{a}\mathfrak{b}),$$

where $\sigma_{\mathfrak{b}} \in \mathrm{Gal}(H/K)$ *is the element corresponding to the ideal class* $\mathfrak{b}$ *via the Artin map.*

Remark 24. If $\mathfrak{a}$ is a primitive ideal in $\mathcal{O}_K$,

$$\mathfrak{a} = \left\langle a, \frac{-b+\sqrt{-d}}{2}\right\rangle_{\mathbb{Z}}$$

with

$$a = N_{K/\mathbb{Q}}(\mathfrak{a})$$
$$b^2 \equiv -D \mod 4a.$$

Moreover

$$j(\mathfrak{a}) = j\left(\frac{-b+\sqrt{-D}}{2a}\right).$$

Goal: Through a similar process, compute $(f(\tau))^\sigma$ for f a modular function and τ a CM point ($A\tau^2 + B\tau + C = 0$ for $A, B, C \in \mathbb{Z}$). We will connect:

(1) automorphism space of the space of modular functions $\mathcal{F}$.
(2) Galois actions: the action of $\mathrm{Gal}(K^{\mathrm{ab}}/K)$ on $f(\tau) \in H \cap K$ for τ a CM point. By this we really many for $x \in \mathbb{A}_K/K^\times$ we associate under the artin map $\sigma_x \in \mathrm{Gal}(K^{\mathrm{ab}}/K)$ and

$$(f(\tau))^{\sigma_x} = f^{x_\tau}(\tau).$$

5.2. **Modular Functions.** Let $\zeta_N = e^{2\pi i/N}$, and write $X(N)$ for the modular curve of level N over $\mathbb{Q}(\zeta_N)$. Note

$$X(N)_{\mathbb{C}} \cong \Gamma(N)\backslash\mathcal{H} \cup \{\text{cusps}\}\,,$$

and the function field is

$$\mathbb{Q}(\zeta_N)(X(N)) =: \mathcal{F}_N = \{\text{modular functions of level } N \text{ with fourier coefficients in } \mathbb{Q}(\zeta_N)\}\,.$$

Definition 25. Modular functions $f : \mathcal{H} \to \mathbb{C}$ are functions satisfying

(1) f is holomorphic on $\mathcal{H}$;
(2) f is invariant under $\Gamma(N)$, that is

$$f\left(\frac{az+b}{cz+d}\right) = f(z)$$

(3) f is 'meromorphic at cusps', roughly meaning that at ∞ the q-expansion satisfies $f(q) = \sum_{n=-m}^{\infty} a_n q^{n/N}$, and similarly at the other cusps.

Example 26. In fact $j \in \mathcal{F}_1$. Moreover if f, g are modular forms of weight k and level N then $f/g \in \mathcal{F}_N$.

(1) $\mathcal{F}_1 = \mathbb{Q}(X(1)) = \mathbb{Q}(j)$;
(2) $\mathcal{F}_N = \mathbb{Q}(\zeta_N) = \mathbb{Q}(j, f_{0,1}, \ldots, f_{1,0})$, where these $f_{i,j}$ are the 'Fricke functions'.

Theorem 27. *$\mathcal{F}_N/\mathcal{F}_1$ is Galois and moreover*

$$\mathrm{Gal}(\mathcal{F}_N/\mathcal{F}_1) \cong \mathrm{GL}_2(\mathbb{Z}/N\mathbb{Z})/\{\pm 1\}\,.$$

Idea of proof. We give the idea. There are two actions in play.

(1) For $f \in \mathcal{F}_N$, we can construct a polynomial (much like in yesterdays lecture)

$$P_f(X) = \prod_{A \in \mathrm{SL}_2(\mathbb{Z})/\Gamma(N)} (X - f(Az)) \in \mathbb{Q}(\zeta_N, j)[X].$$

Here $A \in \mathrm{SL}_2(\mathbb{Z})/\Gamma(N) \cong \mathrm{SL}_2(\mathbb{Z}/N\mathbb{Z})$, and $A \cdot j = f(Az)$
(2) Let $\sigma_d \in \mathrm{Gal}(\mathbb{Q}(\zeta_N)/\mathbb{Q}) \cong \mathbb{Z}/N\mathbb{Z}^\times$ be the automorphism such that $\zeta_N \to \zeta_N^d$. Then

$$f^{\sigma_d}(z) = \sum_{n=-m}^{\infty} a_n^{\sigma_d} q^{n/N}.$$

We embed this in $\mathrm{GL}_2(\mathbb{Z}/N\mathbb{Z})$ via $d \mapsto \begin{pmatrix} 1 & 0 \\ 0 & d \end{pmatrix}$

Note that πI always acts trivially for both of these, which is where the quotient by ± 1 is coming from. $\square$

Let $\mathcal{F} = \cup_{N \geq 1} \mathcal{F}_N$, and then

$$\mathrm{Gal}(\mathcal{F}/\mathcal{F}_1) = \varprojlim \mathrm{GL}_2(\mathbb{Z}/N\mathbb{Z})/\{\pm 1\} = \mathrm{GL}_2(\widehat{\mathbb{Z}})/\{\pm 1\}\,,$$

where $\widehat{\mathbb{Z}} = \prod_{p \nmid \infty} \mathbb{Z}_p$.

Goal: Find $\mathrm{Aut}(\mathcal{F})$. Note that $\mathcal{F}/\mathbb{Q}$ is **not** Galois.

Theorem 28 (Shimura)**.** *There is a short exact sequence*

$$0 \longrightarrow \mathbb{Q}^\times \xrightarrow{\gamma} \mathrm{GL}_2(\mathbb{A}_f) \longrightarrow \mathrm{Aut}(\mathcal{F}) \longrightarrow 1,$$

where $\mathbb{A}_f = \prod'_{p\nmid\infty} \mathbb{Q}_p = \mathbb{A}_\mathbb{Q}/\mathbb{R}$ *is the restricted direct product over only the finite places, and the map* γ *is the diagonal embedding* $a \mapsto \begin{pmatrix} a & 0 \\ 0 & a \end{pmatrix}$.

Action of $\mathrm{GL}_2(\mathbb{A}_f)$ *on* $\mathcal{F}$*:*

$$\mathrm{GL}_2(\mathbb{A}_f) = \mathrm{GL}_2(\mathbb{Q}^+) \cdot \mathrm{GL}_2(\widehat{\mathbb{Z}}),$$

so write $g \in \mathrm{GL}_2(\mathbb{A}_f)$ as γu for $\gamma \in \mathrm{GL}_2(\mathbb{Q}^+)$ and $u \in \mathrm{GL}_2(\widehat{\mathbb{Z}})$. Note that the decomposition above is not unique but

$$f^g = (f^\gamma)^u$$

is well defined. We then have actions of the subgroups via:

- $\mathrm{GL}_2(\mathbb{Q}^+)$ acts by
$$f^\gamma(z) = f(\gamma z);$$
- $\mathrm{GL}_2(\widehat{\mathbb{Z}}) \to \mathrm{GL}_2(\mathbb{Z}/N\mathbb{Z}) \cong \mathrm{SL}_2(\mathbb{Z})/\Gamma(N)$ acts as before $f \mapsto f^u$.

5.3. **Shimura Reciprocity Law.** Recall that $K = \mathbb{Q}(\sqrt{-D})$ for $D > 0$ is an imaginary quadratic field, H the Hilber class field, and $\tau \in H \cap K$. We pick an embedding

$$\begin{aligned} K^* &\to \mathrm{GL}_2(\mathbb{Q}) \\ k &\mapsto g_\tau(k), \end{aligned}$$

where we choose

$$g_\tau(k) \begin{pmatrix} \tau \\ 1 \end{pmatrix} = k \begin{pmatrix} \tau \\ 1 \end{pmatrix}$$

that is, it preserves $\begin{pmatrix} \tau \\ 1 \end{pmatrix} \in \mathbb{P}^1(\mathbb{C})$. Mutatis mutandis, we define an embedding

$$\mathbb{A}_K^\times \to \mathrm{GL}_2(\mathbb{A}_\mathbb{Q}),$$

where now $g_\tau(x) = \begin{pmatrix} t - aB/A & -Cs/A \\ s & t \end{pmatrix}$ where $\tau = s + t\tau$ for $s, t \in \mathbb{A}_\mathbb{Q}$ and $A\tau^2 + B\tau + C = 0$ for some $A, B, C \in \mathbb{Z}$.

Theorem 29 (Shimura)**.** *Let* $f \in \mathcal{F}$ *be a modular function, and* $\tau \in H \cap K$*. For* $x \in \mathbb{A}_K^\times$*,*

$$(f(\tau))^{\sigma_x^{-1}} = f^{g_\tau(x)}(\tau),$$

where:

- $\sigma_x \leftrightarrow x$ *via the Artin map* $\mathbb{A}_K^\times \to \mathrm{Gal}(K^{\mathrm{ab}}/K)$*;*
- $g_\tau(x) \in \mathrm{Aut}(\mathcal{F})$.

Remark 30. $f(\tau) \in K^{\mathrm{ab}}$, and by the theorem we know what the Galois conjugates are.

Example 31. Consider $K = \mathbb{Q}(\sqrt{-3})$, this is a PID, and let $f \in \mathcal{F}_N$ with integer coefficients. Take a primitive ideal

$$\mathcal{A} = \left\langle a, \frac{-b+\sqrt{-3}}{2} \right\rangle_{\mathbb{Z}},$$

where again $a = N_{K/\mathbb{Q}}(\mathcal{A})$ and $b^2 \equiv -3 \mod 4$.

Claim: $f(\tau)^{\sigma_{\mathcal{A}}^{-1}} = f\left(\frac{-b+\sqrt{-3}}{2}\right)$

proof. $\sigma_{\mathcal{A}} = \sigma_x$, where

$$\left(ta + s\frac{-b+\sqrt{-3}}{2}\right) = \mathcal{A} \leftrightarrow \left(ta + s\frac{-b+\sqrt{-3}}{2}\right)_{v|\mathcal{A}} \in \mathbb{A}_K^{\times}.$$

- The minimal polynomial for τ is

$$X^2 + bX + \frac{b^2+3}{4} = 0.$$

Then $g_\tau(x) = \begin{pmatrix} ta - sb & -sca \\ s & ta \end{pmatrix}_{p|\mathcal{A}}$, where $4ac = \frac{b^2+3}{4}$.

Shimura reciprocity gives

$$f(\tau)^{\sigma_x^{-1}} = f^{g_\tau(x)}(\tau).$$

What we do is first write this as a product, that is you can compute that

$$g_\tau(x) = \begin{pmatrix} ta - sb & -sc \\ s & t \end{pmatrix}_{p|\mathcal{A}} \begin{pmatrix} 1 & 0 \\ 0 & a \end{pmatrix}_{p|\mathcal{A}}.$$

It is easy to see that the left hand term is in $\mathrm{SL}_2(\widehat{\mathbb{Z}})$, and has trivial action. We rewrite this right hand side as

$$\begin{pmatrix} 1 & 0 \\ 0 & a \end{pmatrix} \begin{pmatrix} 1 & 0 \\ 0 & a^{-1} \end{pmatrix}_{p\nmid\mathcal{A}}.$$

The right hand side of this acts trivially because the Fourier coefficients are in $\mathbb{Z}$. Thus we get

$$f^{\sigma_{\mathcal{A}}^{-1}}(\tau) = f\left(\frac{\tau}{a}\right).$$

Lecture 5 (Rosu)

6. CM for Elliptic Curves

Today we'll mainly talk about Hecke characters and the theorem of CM for elliptic curves.

Hecke Characters. Let K be a number field, and $\mathbb{A}_K^{\times}$ the idéles. Recall the following definition.

Definition 32. A Hecke character is a continuous homomorphism

$$\chi : \mathbb{A}_K^{\times}/K^{\times} \to \mathbb{C}^{\times}.$$

We write this as $\chi = \otimes_v \chi_v$, where $\chi_v : K_v^{\times} \to \mathbb{C}^{\times}$ is the restriction to the component at the place v. χ has conductor $\mathfrak{f}$ which is the smallest ideal such that $\chi_v(1 + \mathfrak{f}\mathcal{O}_v) = 1$ for all v.

Remark 33. We can think of Hecke characters classically as

$$\chi : I(\mathfrak{f}) \to \mathbb{C}^\times,$$

where the domain here is the ideals prime to $\mathfrak{f}$, with some infinity type (that is, a continuous character $\chi_\infty : K_\infty = K \otimes_\mathbb{Q} \mathbb{R} = \prod_{v|\infty} K_v^\times \to \mathbb{C}^\times$).

Example 34. If $K = \mathbb{Q}(\sqrt{-D})$ an imaginary quadratic field, $\chi_\infty : \mathbb{C}^\times \to \mathbb{C}^\times$ is some continuous homomorphism and for $\alpha \equiv 1 \mod \mathfrak{f} = \mathfrak{f}_\chi$ we have

$$\chi(\langle\alpha\rangle) = \chi_\infty(\alpha)^{-1}$$

Remark 35. If $\chi_\infty = 1$ then we have

$$\chi : I(\mathfrak{f})/\mathcal{P}_{1,\mathfrak{f}} \cong \mathrm{Gal}(H_{(\mathfrak{f})}/K) \to \mathbb{C}^\times,$$

where $H_{(\mathfrak{f})}/K$ is the ray class field for $\mathfrak{f}$. Note that this is a character on a finite group!

We are interested in $\chi_\infty(z) = N_{K/\mathbb{Q}}(z)^{-1} = |z|^{-2}$, which will correspond to elliptic curves.

Remark 36. The two definitions correspond as follows: if $\chi : \mathbb{A}_K^\times/K^\times \to \mathbb{C}^\times$ with conductor $\mathfrak{f}$ is as in the first definition then it corresponds to $\tilde{\chi} : I(\mathfrak{f}) \to \mathbb{C}^\times$ where for a prime $\mathfrak{p} \nmid \mathfrak{f}$ we take

$$\tilde{\chi}(\mathfrak{p}) := \chi_\mathfrak{p}(\pi_\mathfrak{p}),$$

where $\pi_\mathfrak{p}$ is a uniformizer in $K_\mathfrak{p}$, and for the infinite part we take

$$\tilde{\chi}_\infty(z) := \chi_\infty(z).$$

Going back the way we take $\tilde{\chi} : I(\mathfrak{f})/P_{1,\mathfrak{f}} \to \mathbb{C}^\times$ to the character χ with for $\mathfrak{p} \nmid \mathfrak{f}$

$$\chi_\mathfrak{p}(\mathcal{O}_\mathfrak{p}^\times) = 1$$
$$\chi_\mathfrak{p}(\pi_\mathfrak{p}) = \tilde{\chi}(\mathfrak{p})$$

and at $v = \infty$ we take $\chi_\infty = \tilde{\chi}_\infty$.

Example 37 (Dirichlet Characters)**.** $\chi_{Dir} : \mathbb{Z}/N\mathbb{Z}^\times \to \mathbb{C}^\times$ given by $m \mod N \mapsto \zeta^m$, where ζ is an Nth root of unity. Then this corresponds to

$$\begin{aligned} \chi : I_\mathbb{Q}(N) &\to \mathbb{C}^\times \\ \langle p\rangle &\mapsto \chi(p \mod N). \end{aligned}$$

If χ_{Dir} is primitive then the conductor of χ is N. Note that the associated character on the idéles is, for $p \nmid N$:

$$\begin{aligned} \tilde{\chi} : \mathbb{A}_\mathbb{Q}^\times &\to \mathbb{C}^\times \\ \tilde{\chi}_p(p) &= \chi(p \mod N) \\ \tilde{\chi}_\infty(z) &= 1. \end{aligned}$$

Example 38. $K = \mathbb{Q}(\sqrt{-3})$, which is a PID. Then define

$$\varphi : I(3) \to \mathbb{C}^\times,$$

by $\varphi(\langle\alpha\rangle) = \alpha$ for $\alpha \equiv 1 \mod 3$, and let $\varphi_\infty(x) = z^{-1}$. This corresponds to $E : y^2 = x^3 - 432 \leftrightarrow x^3 + y^3 = 1$.

6.1. **Elliptic Curves with CM. Goal:** Finda Hecke character corresponding to χ_E.

Recall from Vonk's lectures

(1) If E/L has CM then $j(E) \in \overline{\mathbb{Z}}$, which is then equivalent to E having potential good reduction at all places of L (meaning that all reduction is either good or additive which becomes good over a finite extension). We have $L_p(E,s) = \begin{cases} \text{good reduction terms} \\ 1 \text{ add reduction} \end{cases}$

(2) If $K = \mathbb{Q}(\sqrt{-D})$ is imaginary quadratic, and $\mathfrak{a} \leq \mathcal{O}_K$ is an ideal, then there is an associated elliptic curve $E = E_{\mathfrak{a}}$ with

$$E_{\mathfrak{a}}(\mathbb{C}) = \mathbb{C}/\mathfrak{a}.$$

Let H/K be the Hilbert class field, then in fact we have $E_{\mathfrak{a}}/H$. Moreover

$$E_{\text{tors}} \cong K/\mathfrak{a}.$$

We have an action of $s \in \mathbb{A}_K^\times$ on E_{tors}

$$\oplus_{\mathfrak{p}} K_{\mathfrak{p}}/\mathfrak{a}_{\mathfrak{p}} \xleftarrow[\sim]{\alpha} K/\mathfrak{a} \xrightarrow{\cdot s} K/s^{-1}\mathfrak{a} \xrightarrow{\sim} \oplus_{\mathfrak{p}} K_{\mathfrak{p}}/s_{\mathfrak{p}}^{-1}\mathfrak{a}_{\mathfrak{p}} \ ,$$

where $\alpha : k \mod \mathfrak{a} \mapsto k \mod fa_{\mathfrak{p}}$.

We now state the main theorem of CM.

Theorem 39 (Main Theorem of CM)**.** *Using the Artin Reciprocity map*

$$\mathbb{A}_K^\times/K^\times \to \mathrm{Gal}(K^{\text{ab}}/K),$$

where we denote the image of s by σ_s, then the Galois action on E_{tors} is given by multiplicationby idéles:

$$\begin{tikzcd} E_{\text{tors}} \cong K/\mathfrak{a} \arrow[r, "s^{-1}"] \arrow[d] & K/s^{-1}\mathfrak{a} \arrow[d] \\ E(L^{\text{ab}}) \arrow[r, "\sigma_s"] & E^{\sigma_s}(L^{\text{ab}}) \end{tikzcd},$$

where $L = \mathbb{Q}(j(E))$, and we think of the top row as 'analytic' and the bottom as 'algebraic'.

6.2. **Hecke Characters for CM Elliptic Curves.**

Theorem 40 (Deuring)**.** *If E/L has CM by $\mathcal{O}_K$ and $K \subsetneq L$ then we can find a Hecke character*

$$\chi_E : \mathbb{A}_{L'}^\times/L'^\times \to \mathbb{C}^\times,$$

where $L' = LK$ is the compositum, such that

$$L(E/L', s) = L(s, \chi_E).$$

Remark 41*.* If $\mathfrak{p}$ is a prime of L then

$$L_{\mathfrak{p}}(E/L', s) = \prod_{\mathfrak{q}|\mathfrak{p}} L_{\mathfrak{q}}(s, \chi_{\mathfrak{q}}).$$

Moreover we have the following.

- Bad reduction corresponds to $\mathfrak{p} \mid \mathfrak{f}$ (where $\mathfrak{f}$ is the conductor f χ_E).

- Good reduction corresponds to 1 on both sides.

Generally this is saying

$$1 - a_{\mathfrak{p}} q^{-s} + q^{1-2s} = \prod_{\mathfrak{q}|\mathfrak{p}} (1 - \chi_E(\mathfrak{q}) N(\mathfrak{q})^{-s}),$$

where $q = N(\mathfrak{p})$.

Remark 42. If $K \subset L$ then $\chi_E : \mathbb{A}_L^\times / L^\times \to K^\times$, and

$$L(E/L', s) = L(s, \chi_E) L(s, \overline{\chi_E}).$$

6.3. **(Idea of) Construction.** The idea of the construction of $\chi_E : \mathbb{A}_L^\times / L^\times \to \mathbb{C}^\times$ in the case $K \subset L$ is as follows.

(1) Construct a homomorphism

$$\begin{aligned} \alpha_E : \mathbb{A}_L^\times \to \mathbb{A}_K^\times \to K^\times \\ x \mapsto N_{L/K}(x) = s \mapsto ? \end{aligned}$$

Recall for E/L with $j(E) \in L$ the diagram from the main theorem of CM:

$$\begin{array}{ccc} K/\mathfrak{a} & \xrightarrow{s^{-1}} & K/s^{-1}\mathfrak{a} \\ \downarrow & & \downarrow \\ E(L^{\mathrm{ab}}) & \xrightarrow{\sigma_s} & E^{\sigma_s}(L^{\mathrm{ab}}) = E(L^{\mathrm{ab}}) \end{array},$$

and note that $s \in N_{L/K} \mathbb{A}_L^\times / L^\times$ if and only if σ_s preserves L, since

$$\mathbb{A}_L^\times / N_{L/K} \mathbb{A}_K^\times / K^\times \cong \mathrm{Gal}(L/K).$$

Thus the bottom line above is an isomorphism and we have that $\mathfrak{a}$ and $s^{-1}\mathfrak{a}$ must be homothetic lattices.

(2) $\chi_E = \alpha_E \cdot (N_{L/K})_\infty^{-1}$

Remark 43. Assume E/H where H is the Hilbert class field of K and E has CM by $\mathcal{O}_K$. Then

(1) $\chi_E : \mathbb{A}_H^\times / H^\times \to K^\times$ determines the isogeny class of E/H.
(2) $(\chi_E, j(E))$ determines the isomorphism class of E/H.
(3) A Hecke character $\chi : \mathbb{A}_H / H^\times \to \mathbb{C}^\times$ correspond to E/H with CM by $\mathcal{O}_K$ if and only if $\chi_\infty = (N_{L/K}^{-1})_\infty$