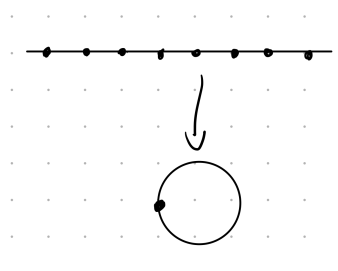
Notation 1. • $\mathbb{Z}' = \mathbb{Z}/\setminus\{0\}$

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

(1) $$\alpha_1^2 = \alpha_2 - 3\Omega_2.$$

- We want a multiplicative lift for

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

  for our function α_1. We take

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

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

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

1.1. **Periods.** Euler realised that

$$\sigma(z) = \sin(\pi z),$$

so that

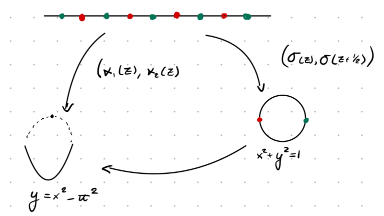
$$\begin{aligned}\alpha_1(z) &= \frac{1}{z} - \sum_{k\geq 2} \Omega_k z^{k-1} \\ &= \pi \cot(\pi z) \\ &= -\pi i (e^{2\pi i z} + 1)/(e^{2\pi i z} - 1).\end{aligned}$$

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 2. 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

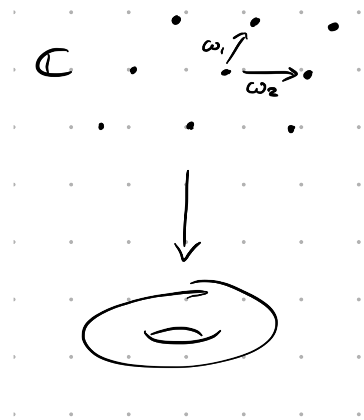
$$\alpha_k(\Lambda, z) = \sum_{\lambda \in \Lambda} \frac{1}{(z-\lambda)^k}.$$

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

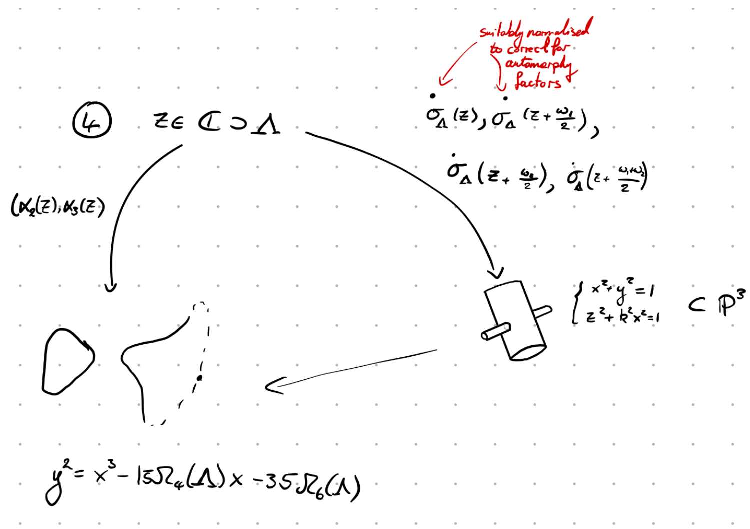
2.1. **Special Values.** The Values at division points of $\mathbb{C}/\Lambda$

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

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

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

Notation 3. Pick coset representatives for

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

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

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

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

3. Singular Moduli

Theorem 4. *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. $\square$

Example 5 (Very Large)**.** See the webpage of Drew Sutherland for many excellent huge examples. Here is a small-ish one.

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

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 6.

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

Moreover $j(\sqrt{-5})$ is a root of $\Phi_5(x)$. Here is a riddle: $j\left(\frac{1+\sqrt{-63}}{2}\right) = -2^{18}3^3 5^3 23^3 29^3 \in \mathbb{Z}$, which polynomial should give this? The answer is 41, try to see this.

Theorem 7 (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

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

$\square$

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 8. 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 9. *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 10. We have

$$\Upsilon_2(x,y) = (x+16)^3 - xy,$$
$$\Upsilon_3(x,y) = (x-9)^3(x-729) + 72x(x+21)y - xy^2.$$

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 11. *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 $\langle \lambda_1 \ldots \lambda_f\rangle = \overline{\mathfrak{p}}^{12}$. Thus $\langle\lambda_i\rangle = \overline{\mathfrak{p}}^{12}$.

Theorem now follows from

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

□