Modular Forms

§0. Some motivation and background

In this course we will study the most classical "automorphic forms" namely (elliptic) modular forms.

They can be thought as a generalization of periodic functions.

Let's begin with the definition of periodic functions on $\mathbb{R}$.

A function $f: \mathbb{R} \to \mathbb{C}$ is <u>periodic</u> with period, say 1, if

$$(*) \quad f(x+1) = f(x) \qquad \forall x \in \mathbb{R}$$

In fact $(*)$ implies that $f(x+n) = f(x)$ $\forall n \in \mathbb{Z}, \forall x \in \mathbb{R}$

Recall the group $\mathbb{Z}$ acts on $\mathbb{R}$ by translation

$$\cdot \quad \mathbb{Z} \times \mathbb{R} \longrightarrow \mathbb{R}$$
$$(n, x) \longmapsto n \cdot x := n + x$$

and the periodic function f is just a function which is invariant under this action.

A very powerful tool in studying periodic functions is Fourier analysis, which is Harmonic analysis on $\mathbb{R}/\mathbb{Z}$.

The question / problem is to express any periodic, "reasonably nice" function in terms of "simple" ones.

Note the set of all periodic functions is a vector space, and there is an inner product defined on it by

$$\langle f, g \rangle := \int_0^1 f(x)\overline{g(x)}\,dx$$ (at least for nice f, g)

We are looking for an orthonormal basis $e_n(x)$ of such functions so that

$f(x) = \sum a_n e_n(x)$ where

$a_n = \int_0^1 f(x)\overline{e_n(x)}\,dx$.

One such choice is $e_n(x) = e^{2\pi i n x}$, which leads to the exponential Fourier series. The good basis above arises as eigenfunctions of a differential operator, namely the Laplace operator

$$\Delta = \frac{d^2}{dx^2}$$

Side note: The original problem which motivated Fourier was finding the general soln for the heat equation in a thin plate. It was known that if the heat source was expressible as a sinusoidal wave, then the solution was similarly expressible as a sinusoidal wave. The idea was to use a superposition of waves to attack the problem for an arbitrary heat source.

—o—

This semester we will study functions not on $\mathbb{R}$ but on $\mathbb{H}$ = upper half plane which will be invariant or transforming in a prescribed way with respect to the action of a group on $\mathbb{H}$, namely the group $SL(2, \mathbb{Z})$ of 2×2 integer matrices of det 1, (or its s/groups) by Linear Fractional transformations.

We can ask various regularity conditions on such functions. We can ask for example that ① They are holom on $\mathbb{H}$ or ② " meromorphic on $\mathbb{H}$

or (3) Eigenfunctions of some diff. operator namely the corresponding Laplacian.

(f) We will ask some conditions on the growth of $f : \mathbb{H} \to \mathbb{C}$ as $\tau \in \mathbb{H}$ goes to ∞.

We'll start with the strongest regularity conditions and depending on time we will look at other classes of functions.

The course is called <u>modular forms</u>

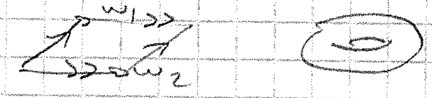
We can start by asking where the <u>word</u> modular is coming from?

<u>Modular</u> refers to the <u>moduli</u> space of complex curves of genus one.

A complex curve of genus 1 arises from a lattice Λ in $\mathbb{C}$ as $\mathbb{C}/\Lambda$. A lattice Λ is a set

$\Lambda = \mathbb{Z}\omega_1 + \mathbb{Z}\omega_2$ with $\{\omega_1, \omega_2\}$ a basis of $\mathbb{C}$ over $\mathbb{R}$

This is a complex torus: $\mathbb{C}/\Lambda = \{z + \Lambda \mid z \in \mathbb{C}\}$

Quotient of $\mathbb{C}$ by Λ 

(It is also $S^1 \times S^1$

Algebraically, it is also an Abelian group under addition (inherited from $\mathbb{C}$)

But it also has a complex structure (also inherited from $\mathbb{C}$), i.e.

It is a Riemann surface, connected 1 dimensional complex manifold.

(It is a connected Hausdorff space, which is endowed with an atlas of charts to the open unit disc of $\mathbb{C}$ with transition maps between two overlapping charts are holomorphic)

$\mathbb{C}/\Lambda$ is a <u>compact</u> Riemann surface.

For two different tori $\mathbb{C}/\Lambda$, $\mathbb{C}/\Lambda'$ we have the following theorem

<u>Prop</u> Suppose $\varphi : \mathbb{C}/\Lambda \to \mathbb{C}/\Lambda'$ is a holomorphic map between complex Tori. Then $\exists$ complex numbers $a, b \in \mathbb{C}$ with $a\Lambda \subset \Lambda'$ such that $\varphi(z+\Lambda) = az + b + \Lambda'$. The map is invertible if and only if $a\Lambda = \Lambda'$

(For a proof see for example Diamond-Schurmann Prop 1.3.2) or Complex Functions by Jones-Singerman Thm 4.18.)

When we say 2 complex curves of genus 1 are isomorphic, we mean that there is a holom map between them which is invertible. So the above Prop. says that $\mathbb{C}/\Lambda_1 \cong \mathbb{C}/\Lambda_2 \iff \Lambda_1 = \lambda \Lambda_2$ for some $\lambda \in \mathbb{C}^*$

We say 2 lattices are equivalent (homothetic) $\Lambda_1 \sim \Lambda_2$ iff $\Lambda_1 = \lambda \Lambda_2$ for some $\lambda \in \mathbb{C}^*$.

Any lattice $\Lambda = \mathbb{Z}\omega_1 + \mathbb{Z}\omega_2 = \omega_2\left(\mathbb{Z}\left(\frac{\omega_1}{\omega_2}\right) + \mathbb{Z}\right)$

is equivalent to a lattice of the form

$$\Lambda_\tau = \mathbb{Z}\tau + \mathbb{Z} \quad \text{w/} \quad \tau = \omega_1/\omega_2$$

In fact we can assume $\tau = \frac{\omega_1}{\omega_2} \in \mathbb{H} = \{x+iy \mid y>0\}$

since $\Lambda_\tau \cong \Lambda_{-\tau}$.

From now on assume $\operatorname{Im}\left(\frac{\omega_1}{\omega_2}\right) > 0$

$$\left(\det \begin{pmatrix} \operatorname{Re}\omega_2 & \operatorname{Im}\omega_2 \\ \operatorname{Re}\omega_1 & \operatorname{Im}\omega_1 \end{pmatrix} > 0 \right).$$

We also have:

<u>Lemma</u> $\Lambda(\omega_1, \omega_2) = \Lambda(\omega_1', \omega_2')$
$\Leftrightarrow \exists\; a, b, c, d \in \mathbb{Z}$, $ad - bc = \pm 1$
such that

$$\begin{pmatrix} \omega_1' \\ \omega_2' \end{pmatrix} = \begin{pmatrix} a & b \\ c & d \end{pmatrix} \begin{pmatrix} \omega_1 \\ \omega_2 \end{pmatrix}$$

Moreover if $\operatorname{Im} \frac{\omega_1}{\omega_2} > 0$ then $\operatorname{Im}\left(\frac{\omega_1'}{\omega_2'}\right)$ has the same sign as $ad - bc$.

Note this lemma also says that the set $M = \{ (\omega_1, \omega_2) \in \mathbb{C}^2 \mid \operatorname{Im} \frac{\omega_1}{\omega_2} > 0 \}$ is acted upon by $SL_2(\mathbb{Z})$ via $\gamma \cdot (\omega_1, \omega_2) := (a\omega_1 + b\omega_2, c\omega_1 + d\omega_2)$

and the set of all lattices

$$\mathcal{L} = \{ \Lambda(\omega_1, \omega_2) = \mathbb{Z}\omega_1 + \mathbb{Z}\omega_2 \mid \{\omega_1, \omega_2\} \text{ basis of } \mathbb{C}/\mathbb{R} \}$$

can be identified with the quotient

$$SL_2(\mathbb{Z}) \backslash M$$

Now consider a function $F : \mathcal{L} \to \mathbb{C}$ on lattices. Such a function is called <u>modular</u> if $F(\Lambda_1) = F(\Lambda_2)$ whenever

$$\Lambda_1 = \lambda \Lambda_2 \quad \text{for some } \lambda \in \mathbb{C}^*$$

Since by the above Prop

$$\mathbb{C}/\Lambda_1 \cong \mathbb{C}/\Lambda_2 \quad \text{whenever } \Lambda_1 = \lambda \Lambda_2$$

A modular function on lattices is a function on complex curves of genus I.

Since any lattice $\Lambda(w_1, w_2) \sim \Lambda_\tau$ for some $\tau \in \mathbb{H}$, the function F is completely determined by its values on $f(\tau) := F(\mathbb{Z}\tau + \mathbb{Z}) = F(\Lambda_\tau)$

The change of basis $\begin{pmatrix} w_1' \\ w_2' \end{pmatrix} \mapsto \begin{pmatrix} a & b \\ c & d \end{pmatrix} \begin{pmatrix} w_1 \\ w_2 \end{pmatrix}$

w/ $\begin{pmatrix} a & b \\ c & d \end{pmatrix} \in SL_2(\mathbb{Z})$ translate for f

into a <u>modular invariance</u> property

$$f\left(\frac{a\tau + b}{c\tau + d}\right) = f(\tau)$$

For many applications invariance is too restrictive and instead one considers functions on lattices which are homogeneous

$F: \mathcal{L} \to \mathbb{C}$ is called homogeneous of degree $-k$ if

$$F(\lambda\Lambda) = \lambda^{-k} F(\Lambda)$$

We then have

Lemma Let $F: \mathcal{L} \to \mathbb{C}$ homog of degree $-k$. Then the function

$f: \mathbb{H} \to \mathbb{C}$ defined as

$f(\tau) = F(\Lambda(\tau, 1))$ satisfies

$$(*) \quad \boxed{f\left(\frac{a\tau+b}{c\tau+d}\right) = (c\tau+d)^{+k} f(\tau) \quad \forall \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \Gamma}$$

This correspondence is a bijection.

(Given f which satisfies $(*)$ define

$$F(\Lambda(\omega_1, \omega_2)) := \omega_2^{-k} f\left(\frac{\omega_1}{\omega_2}\right)$$
)

Proof Exercise

The defn of function $f: \mathbb{H} \to \mathbb{C}$ which satisfy (*) plus some regularity conditions many not look very natural at first sight but they arise "naturally" in a variety of subjects in math and physics and these functions often encode arithmetic, geometric, combinatorial information.

We start with the most basic such functions which have strong regularity conditions

<u>Defn</u> $f: \mathbb{H} \to \mathbb{C}$ is called <u>a modular form of wt $k \in \mathbb{N}$ for $\Gamma := SL(2,\mathbb{Z})$</u> if

a) f is holom. on $\mathbb{H}$ $\quad \left(\frac{\partial}{\partial \bar{z}} f = 0\right)$

b) $f(\gamma\tau) = (c\tau + d)^k f(\tau) \quad \forall \begin{pmatrix} a & b \\ c & d \end{pmatrix} = \gamma \in \Gamma$

and $\gamma\tau := \dfrac{a\tau + b}{c\tau + d}$

c) f is "holomorphic at ∞".

If we choose $\gamma = \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}$ then

b) $\Rightarrow f(\tau + 1) = f(\tau)$

and f holom on $\mathbb{H}$ $\Rightarrow$

$$\underline{f(z) = \sum_{n \in \mathbb{Z}} a(n) e^{2\pi i n z}}$$

f holom at ∞ means that
$a(n) = 0$ for $n < 0$

Q: What is an example of a modular form?

A: The prime examples are the so called
Θ_functions.
The simplest one of these does not actually fit into our simplest definition in the sense that they are modular forms for a subgroup of Γ in general, and their weight k is not an integer in general but half an integer.
Nevertheless, for the purpose of motivation, let's look at the simplest Θ_function and see why a number theorist might care to study such a function.

The simplest $\underline{\Theta\text{-function}}$ is defined as $\Theta(z) = \sum_{n \in \mathbb{Z}} e^{2\pi i n^2 z} = \sum_{n \in \mathbb{Z}} e(n^2 z)$

$e(x) := e^{2\pi i x}$.

Clearly $\theta(\tau+1)=\theta(\tau)$ θ_n 12

$$\theta(\tau)=\sum_n e(n^2\tau)=1+\sum_{n=1}^{\infty}2e^{2\pi i n^2\tau}$$

if

$$\theta(\tau)=\sum a(m)e^{2\pi i m\tau}$$

then its m-th Fourier coef is either 1, 2 or 0 depending on whether m is zero, a square or non-square resp.

ie $a(m)=\begin{cases}1 & \text{if } m=0\\ 2 & \text{if } m=\square\\ 0 & \text{o.w.}\end{cases}$

Not too interesting but neverthless θ carries some arithmetic information in its Fourier coefficients.

To make it more interesting, lets look at its s-th power

$$\theta^s(\tau)=\sum_{n_1\in\mathbb{Z}}\sum_{n_2\in\mathbb{Z}}\cdots\sum_{n_s\in\mathbb{Z}}e^{2\pi i(n_1^2+\cdots+n_s^2)\tau}$$

$$=1+\sum_m r_s(m)e^{2\pi i m\tau}$$

where $r_s(m):=\#\{(n_1,\ldots,n_s)\in\mathbb{Z}^s \mid n_1^2+\cdots+n_s^2=m\}$

Here we count reps distinct even if order or the sign is changed.

eg $r_2(5)=8$ since $5=(\pm2)^2+(\pm1)^2$
$=(\pm1)^2+(\pm2)^2$

$\Theta^s(\tau)$ is a generating function for the representation numbers of sums of squares.

Q. How does this help or does it help to understand $r_s(m)$?

A. In general the "effectiveness" of modular forms in the study of arithmetic problems is due to the fact that the space

$$M_k(\Gamma) := \{ f : \mathbb{H} \to \mathbb{C} \mid f \text{ is a mod. form of wt } k \text{ for } \Gamma \}$$

is a finite dim'l vector space.

Hence suppose you know that $\dim M_k(\Gamma) = 1$ for some k (This is the case for example when $k=4$). And suppose you have found 2 different functions coming from different sources, f, and g both are in $M_k(\Gamma)$. Then we know that $f = \alpha g$ for some $\alpha \in \mathbb{C}$

if $f = \sum a_n e(n\tau)$ $\quad g = \sum b_n e(n\tau)$

Then $a_n = \alpha b_n$ $\forall n$ and $\alpha = a_0 / b_0$

if $b_0 \neq 0$

In fact this is precisely what is behind the famous formulas of Jacobi for sums of 2, 4, 6, 8 squares

Thm (Jacobi (1804 – 1851))

① $$r_2(m) = 4 \sum_{d \mid m} \chi_{-4}(d)$$

where $\chi_{-4}(d) = \begin{cases} 1 & \text{if } d \equiv 1\ (4) \\ -1 & d \equiv 3\ (4) \\ 0 & \text{else} \end{cases}$

② $$r_4(m) = 8\,(2 + (-1)^m) \sum_{\substack{d \mid m \\ d \text{ odd}}} d > 0$$

(Since d is at least 1.)

③ $$r_6(m) = 16 \sum_{d \mid m} d^2 \chi_{-4}\left(\frac{m}{d}\right) - 4 \sum_{d \mid m} d^2 \chi_{-4}(d)$$

Cor (Lagrange) $r_4(m) > 0$ for any $m > 0$.
Ie every +ve integer m can be represented as a sum of 4 squares.

Rk Jacobi's thm gives a quantitative version of Lagrange's thm.

Sums of squares $x_1^2 + \dots + x_s^2 = Q(x)$
is the simplest quadratic form (simplest lattice)
More general θ-functions attached to quadratic forms (or equivalently lattices)

can be defined

let $Q : \mathbb{R}^n \longrightarrow \mathbb{R}$

$$(x_1, \dots x_n) \longmapsto Q(x_1, \dots x_n) = \sum_{i,j} a_{ij} x_i x_j$$

be an integral quadratic form, ie $Q(x) \in \mathbb{Z}$ if $x \in \mathbb{Z}^n$. For any $x \in \mathbb{R}^n$

$Q(x) = x A x^t$ for some $A = (a_{ij})$ sym matrix. We'll assume A is positive definite.

The <u>theta function</u> attached to Q

is $\theta_Q(\tau) = \sum_{x \in \mathbb{Z}^n} q^{Q(x)}$

$$= 1 + \sum_{m=1}^{\infty} N_m q^m$$

where $N_m = \# \{ x \in \mathbb{Z}^n \mid x A x^t = m \}$.

and $q = e^{\pi i \tau}$.

Equivalently we can associate to a lattice $\Lambda = \mathbb{Z}v_1 + \dots + \mathbb{Z}v_n \in \mathbb{R}^n$ w/ $\{v_1, \dots v_n\}$ a basis of $\mathbb{R}^n$, a θ-series $\theta_\Lambda(\tau)$ as follows.

Any $l \in V$ is of the form $l = x_1 v_1 + \dots x_n v_n$

let $M = \begin{pmatrix} v_1 & \text{---} \\ v_2 & \text{---} \\ v_n & \text{---} \end{pmatrix}$ Then for any $l \in \Lambda$

$$\langle l, l\rangle = x M M^t x^t = x A x^t \quad \text{with}$$

$$A = M M^t, \quad x = (x_1 \cdots x_n)$$

Define $\vartheta_\Lambda(\tau) := \sum_{l \in \Lambda} q^{\langle l, l\rangle}$

$$= 1 + \sum N_m q^m$$

$$N_m := \#\{ l \in \Lambda \mid \langle l, l\rangle = m \}$$

$$= \#\{ x \in \mathbb{Z}^n \mid x A x^t = m \}$$

as before.

These functions also have applications to the sphere packing problem.

Sphere Packing Problem

If one has a lattice $\Lambda \subset \mathbb{R}^n$ and put a sphere at each lattice point to pack $\mathbb{R}^n$ w/ spheres, then density of the packing $\Delta_\Lambda = \begin{pmatrix}\text{volume of} \\ \text{the sphere}\end{pmatrix} \begin{pmatrix}\text{density of} \\ \Lambda\end{pmatrix}$

density of Λ = average # of points per unit volume

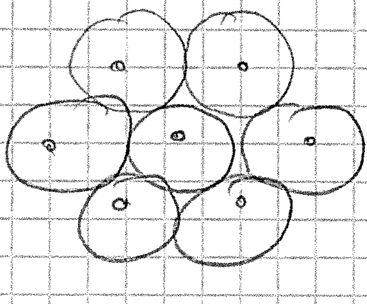
Clearly the largest sphere we can put (without overlaps) is determined by ρ

$$\rho = \underset{\text{in } \Lambda}{\text{min distance}} = \min\{ |l| = \langle l, l\rangle^{1/2} \mid l \in \Lambda \}$$

What is the densest sphere packing in $\mathbb{R}^n$?

$n=1$, $\Delta = 1$ $[\ \mathbb{Z}\ ]$

$n=2$ $\Delta = \frac{\pi}{3\sqrt{2}} \approx 0.74$ (Gauss)



given by Hexagonal lattice

$n=3$ $\Delta = \frac{\pi}{\sqrt{18}}$ given by face centered cubic

(Kepler's problem)

A pf. announced by Hales in 1998 completed in 2014.

For $n \geq 4$ it was a wide open problem until recently

In 2016, Viazovska proved that in $\dim = 8$

$$\Lambda = E_8 = \{ v = \sum a_i e_i \in \mathbb{Z}^8 \cup (\mathbb{Z} + \tfrac{1}{2})^8 \mid \sum a_i = \text{even} \}$$

gives the densest packing

Followed immediately by

$n=24$ $\Lambda =$ Leech lattice is the densest

Proved by H. Cohn, A. Kumar, S. Miller, D. Radchenko, M. Viazovska.

The proof uses the theory of mod. forms together with linear programming bounds.

For lattice packings density of $\Lambda = \frac{1}{\det M}$

where $M = \begin{pmatrix} v_1 & - & - \\ \vdots \\ v_n & - & - \end{pmatrix}$ $\{v_1, \ldots, v_n\}$ a basis of Λ.

$$\Delta_\Lambda = \begin{pmatrix} \text{vol of ball of} \\ \text{radius } \rho/2 \end{pmatrix} \begin{pmatrix} \text{density of} \\ \Lambda \end{pmatrix}.$$

$$\left(\frac{\pi^{n/2}}{\Gamma(\frac{n}{2}+1)} (\rho/2)^2 \right) \left(\frac{1}{\det M} \right)$$

For large n, we know no feasible way to compute the minimal length of a general lattice given its generators.

We first change the problem to a seemingly harder one and ask not only for minimal length but also for all lengths.

Equivalently we ask for the generating function for the squares of all lengths in Λ.

$$\vartheta_\Lambda(q) = \sum_{l \in \Lambda} q^{\langle l, l \rangle} = 1 + \sum N_m q^m$$
$$= 1 + K q^{\rho^2} + \ldots$$

First non-zero Fourier coef (after 1) gives the square of ρ in the power and the <u>Kissing # K</u> as coeff.

K = # of lattice vectors of minimal length

<u>Ex</u> in $n=8$, θ_{E_8} is actually a mod form of wt 4 for $SL_2(\mathbb{Z})$

$\theta_{E_8} \in M_4(\Gamma)$. There is another wt 4 form (which we'll see soon), the so called Eisenstein series

$$G_4(\tau) = 1 + 240 \sum_m \sigma_3(m) e^{2\pi i m \tau}$$

where $\sigma_3(m) = \sum_{d \mid m} d^3$

But $\dim M_4(\Gamma) = 1$ Hence

$$1 + Kq^{\rho^2} + \dots = \theta_{E_8} = G_4 = 1 + 240 q^2 + \dots$$

$$\Rightarrow \rho^2 = 2, \quad K = 240$$

Ie Min length is $\sqrt{2}$ attained by 240 vectors : $\left(\begin{array}{ll} 112 \text{ vectors} & \pm e_i \pm e_j \\ 128 \quad " & \frac{1}{2} \sum a_j e_j \\ & \text{w/ } a_j = \pm 1 \\ & \prod a_j = 1 \end{array} \right)$

See : Conway Sloane Lattices and Sphere Packings

Rk ① Different lattices can give rise to the same Θ-function.
eg. in 16 dimensions there are 2 inequivalent unimodular ($\det M = 1$) lattices D_{16}, $E_8 \oplus E_8$ but

$$\Theta_{D_{16}} = \Theta_{E_8 \oplus E_8}.$$

This is intimately connected to the question
"Can you hear the shape of a drum?"

Two manifolds induced by 2 quadratic forms are non-isom but isospectral (ie have the same spectrum for the associated Laplacian)

② Jacobi studied more general Θ functions functions of 2 variables: $\tau \in \mathbb{H}$, $z \in \mathbb{C}$

$$\Theta(\tau, z) := \sum_{n \in \mathbb{Z}} e^{2\pi i n z} e^{\pi i n^2 \tau}$$

$\Theta(it, x)$ is a soln of the heat eqn in $\mathbb{R}/\mathbb{Z}$ ($t \in \mathbb{R}^+$, $x \in \mathbb{R}$)

$$\frac{\partial}{\partial t} \Theta = \frac{1}{4\pi} \frac{\partial^2}{\partial x^2} \Theta$$

$\vartheta(\tau, z)$ satisfy the following transformations

(a) $\vartheta(\tau+2, z) = \vartheta(\tau, z)$

(b) $\vartheta(\tau, z+\tau) = e^{-2\pi i z - \pi i \tau} \, \vartheta(\tau, z)$

Functions which satisfy similar transformation properties are now called Jacobi modular forms and appear in a lot of problems in Physics and geometry.

Probably the most exiting application of θ to Number theory is its relation to the Riemann zeta function

$$\zeta(s) = \sum_{n=1}^{\infty} \frac{1}{n^s} = \prod_p (1-p^{-s})^{-1} \quad \mathrm{Re}\, s > 1$$

is a prototype of a Dirichlet series with an Euler product.

It is known that $\Lambda(s) := \pi^{-s/2} \, \Gamma\left(\frac{s}{2}\right) \zeta(s)$

then $\Lambda(s)$ has merom. continuation to all $\mathbb{C}$ except for simple poles at $s=1, 0$ and satisfies the Func'l eqn $\Lambda(s) = \Lambda(1-s)$

What is the relation between θ and ξ?

$$\Lambda(2s) = \int_0^\infty \frac{1}{2}\left(\theta\left(\frac{it}{2}\right) - 1\right) t^s \, \frac{dt}{t}$$

Λ is the "Mellin transform" of θ

θ satisfies (a) $\theta(\tau+1) = \theta(\tau)$

(b) $\theta\left(-\frac{1}{4\tau}\right) = \sqrt{\frac{2\tau}{i}}\, \theta(\tau)$

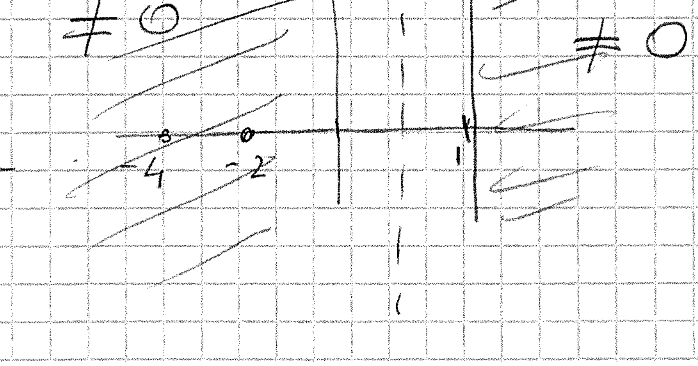
$\sqrt{\ }$: argument in RHP

We'll see that (b) $\Longrightarrow$ Analy. cont. and func'l eqn of $\xi(s)$

Since $\xi(s) = \prod (1-p^{-s})^{-1}$ $\quad \mathrm{Re}\, s > 1$

For $\mathrm{Re}\, s > 1$, $\xi(s) \neq 0$

By F.E. this gives that $\xi(s) \neq 0$ for $\mathrm{Re}\, s < 0$ except for simple zeros at $s = -2, -4, \ldots$ coming from the poles of Γ-function.



RH: If $s \neq -2, -4, \ldots$ and $\xi(s) = 0$ then $\mathrm{Re}\, s = \frac{1}{2}$

$(s \neq -2, -4, \ldots)$

Rk: The relation between $\zeta(s) \longleftrightarrow \Theta(z)$

is a prototype of the relation between

$$\left\{\begin{array}{l}\text{zeta, } L\text{-functions} \\ \sum a_n n^{-s} \\ \text{with AC and FE}\end{array}\right\} \longleftrightarrow \left\{\begin{array}{l}\text{modular} \\ \text{(automorphic} \\ \text{forms}\end{array}\right.$$

Rk ① $\zeta(1+it) \neq 0 \quad t \in \mathbb{R}$ (i.e. pushing the non-vanishing to $\mathrm{Re}\, s = 1$)

$\Rightarrow$ PNT Prime Number Theorem

$$\pi(x) = \#\{p \text{ prime} \mid p \leq x\} \sim \frac{x}{\ln x}$$

② $\zeta(1-n) = (-1)^n B_{n+1}/n+1$

$$\zeta(2r) = (-1)^{r-1} B_{2r} \frac{(2\pi)^{2r}}{2(2r)!}$$

$$\zeta(-1) = -1/12, \quad \zeta(0) = -1/2$$

We know ζ at negative integers

ζ at +ve even integers

But ζ at odd +ve integers are mysteries

$\zeta(3)$ is irrational (Apéry)

B_n's are the Bernoulli #s.

$$\frac{t}{e^t - 1} = \sum_{m=0}^{\infty} \frac{B_m t^m}{m!}.$$

$(B_{2k+1} = 0 \quad \text{for } k > 0)$

(3) The convergence of the Euler product $\prod_p (1-p^{-s})^{-1}$ $\operatorname{Re} s > 1$

is equivalent to the convergence of the series $\sum_p p^{-s}$.

The pole of $\zeta(s)$ at $s=1 \Rightarrow \sum \frac{1}{p}$ diverges

This in return implies there are

∞ly many primes!

<u>Coming attraction:</u> (1) We'll see that

modularity of $\Theta \Rightarrow$ A.C and F.E of ζ

Similarly given a modular form

$f = \sum a_n e(n\tau)$ one can associate

a Dirichlet series $L(f,s) = \sum a_n n^{-s}$

mod. of $f \Longrightarrow$ A.C. and funct'l eqn of $L(f,s)$

$= L(\theta, s)$

0. 25

(2) $\xi(s)$ has an Euler product

Is this true for any $L(f, s)$

No! In general NO!

But we'll see that it is the case if f is an eigenfunction of certain operators $T_n : M_k \to M_k$ $\forall n$, and the space $M_k(\Gamma)$ has a basis consisting of such functions.

Finally The tradition of determining whether a Dirichlet series $\sum \frac{a_n}{n^s}$ has meromorphic continuation to $\mathbb{C}$ and computing its special values or residues at poles has a very long and rich history. For example

Another such thm is Dirichlet's thm on primes in arithmetic progressions.

Let $m > 0$ be given, and $a < m$, $(a, m) = 1$

Consider the progression

$\{a, a+m, a+2m, \dots\}$

<u>Question</u> Are there ∞ly many primes in this list?

How are they distributed.

Let $P_a = \{ p \mid p \equiv a \mod m \}$

<u>Dirichlet's thm</u> ① $\exists$ ∞ly many primes in any P_a

② The $\phi(m)$ disjoint sets contain asymp equally many primes

Dirichlet's thm is a consequence of the fact that

$$\lim_{s \to 1} L(\chi_m, s) \neq 0 \quad \text{where}$$

$\chi_m : \mathbb{Z}/m\mathbb{Z} \longrightarrow \mathbb{C}$ is a character extended to all $\mathbb{Z}$ by

$$\chi(n) = \begin{cases} \chi(n \bmod m) & \text{if } (n,m) = 1 \\ 0 & \text{else} \end{cases}$$

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

There are other sources of L functions

- Number fields
- Galois repns

$$\rho : G = Gal(E/K) \to GL_n$$

- Geometric eg. attached to Elliptic curves

Let E be a curve $/\mathbb{Q}$ given by Weierstrass eqn $y^2 = x^3 + Ax + B = g(x)$ with disc $\Delta = -16(4A^3 + 27B^2)$

For $A, B \in \mathbb{Z}$, $\Delta \neq 0$ consider for each prime p, the reduced curve $E/\mathbb{F}_p$.

Let $N_p = \#$ of points on $E/\mathbb{F}_p$

It turns out that N_p is well approximated by p. More precisely the difference

$$p - N_p =: a_p \text{ satisfy}$$

$$|a_p| < 2\sqrt{p} \quad \text{Hasse}$$

In order to understand how a_p vary with p Hasse began, Weil continued to investigate the L-function for E which is defined by an Euler product

$$L(E,s) = \prod_{p\mid\Delta} (\quad)^{-1} \prod_{p\nmid\Delta} \left(1 - a_p p^{-s} + p^{1-2s}\right)^{-1}$$

<u>Conjecture</u> (Hasse - Weil) $L(E,s)$ has AC to an entire function and satisfy $\Lambda(E,s) = \Lambda(E, 2-s)$

This conjecture is now a thm due to Wiles, Wiles - Taylor

<u>Conjecture</u> Shimura - Taniyama - Weil

Let $f(z) = \sum a_n e(nz)$ Then f is a cusp form of wt 2 for some s/gp of Γ.

(Here a_n's are obtained from a_p multiplicatively, a_p as above $= p - N_p$)

This is also now a thm due to Wiles Breuil - Conrad - Diamond - Taylor

<u>Thm</u> (Frey - Serre - Ribet)

STW conjecture $\Rightarrow$ Fermat's last thm

<u>Cor</u> (Wiles) Fermat's last thm holds.