# Modular forms and their applications I

**Danylo Radchenko**

ETH Zurich

August 24, 2020

Online Summer School on Optimization, Interpolation and Modular Forms
August 24-28, 2020, EPFL

# The notion of modular forms

Let $\mathbb{H} = \{\tau \in \mathbb{C} \colon \operatorname{Im} \tau > 0\}$ be the complex upper half-plane.

# The notion of modular forms

Let $\mathbb{H} = \{\tau \in \mathbb{C} : \operatorname{Im} \tau > 0\}$ be the complex upper half-plane.

A modular form (of weight $k$) on $SL_2(\mathbb{Z})$ is an analytic function $f : \mathbb{H} \to \mathbb{C}$ satisfying

$$f\left(\frac{a\tau + b}{c\tau + d}\right) = (c\tau + d)^k f(\tau)\,, \qquad \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in SL_2(\mathbb{Z}) \tag{i}$$

that has a convergent Fourier expansion of the form

$$f(\tau) = \sum_{n \geq 0} a_n q^n\,, \qquad q := e^{2\pi i \tau} \tag{ii}$$

## The notion of modular forms

Let $\mathbb{H} = \{\tau \in \mathbb{C} \colon \operatorname{Im}\tau > 0\}$ be the complex upper half-plane.

A modular form (of weight $k$) on $\mathrm{SL}_2(\mathbb{Z})$ is an analytic function $f\colon \mathbb{H} \to \mathbb{C}$ satisfying

$$f\left(\frac{a\tau + b}{c\tau + d}\right) = (c\tau + d)^k f(\tau)\,, \qquad \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \mathrm{SL}_2(\mathbb{Z}) \tag{i}$$

that has a convergent Fourier expansion of the form

$$f(\tau) = \sum_{n \geq 0} a_n q^n\,, \qquad q := e^{2\pi i \tau} \tag{ii}$$

If $a_0 = 0$, $f$ is called a cusp form. We denote by $M_k(\mathrm{SL}_2(\mathbb{Z}))$ and $S_k(\mathrm{SL}_2(\mathbb{Z}))$ the spaces of modular forms and cusp forms of weight $k$ respectively.

# Moduli space of genus 1 curves

If $f(\frac{a\tau+b}{c\tau+d}) = f(\tau)$ and $f(\tau) = \sum_{n>-c} a_n q^n$, $f$ is called a modular function.

# Moduli space of genus 1 curves

If $f(\frac{a\tau+b}{c\tau+d}) = f(\tau)$ and $f(\tau) = \sum_{n>-c} a_n q^n$, $f$ is called a modular function.

The name "modular" comes from the fact that one can define a function on lattices

$$\Lambda = \mathbb{Z}\omega_1 + \mathbb{Z}\omega_2 \quad \mapsto \quad F(\Lambda) := f(\omega_1/\omega_2)\,,$$

and since $F(\lambda\Lambda) = F(\Lambda)$, $F(\Lambda)$ is an invariant of the complex curve $\mathbb{C}/\Lambda$.

# Moduli space of genus 1 curves

If $f(\frac{a\tau+b}{c\tau+d}) = f(\tau)$ and $f(\tau) = \sum_{n>-c} a_n q^n$, $f$ is called a modular function.

The name “modular” comes from the fact that one can define a function on lattices

$$\Lambda = \mathbb{Z}\omega_1 + \mathbb{Z}\omega_2 \quad \mapsto \quad F(\Lambda) := f(\omega_1/\omega_2)\,,$$

and since $F(\lambda\Lambda) = F(\Lambda)$, $F(\Lambda)$ is an invariant of the complex curve $\mathbb{C}/\Lambda$.

By analogy, if $f$ is a modular form of weight $k$, then

$$\Lambda = \mathbb{Z}\omega_1 + \mathbb{Z}\omega_2 \quad \mapsto \quad F(\Lambda) := \omega_2^{-k} f(\omega_1/\omega_2)\,,$$

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

# Other groups

One may also consider functions that satisfy $f(\frac{a\tau+b}{c\tau+d}) = (c\tau+d)^k f(\tau)$ only for $\begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \Gamma$, where $\Gamma$ is a subgroup of finite index in $\mathrm{SL}_2(\mathbb{Z})$.

# Other groups

One may also consider functions that satisfy $f(\frac{a\tau+b}{c\tau+d}) = (c\tau+d)^k f(\tau)$ only for $\begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \Gamma$, where $\Gamma$ is a subgroup of finite index in $\mathrm{SL}_2(\mathbb{Z})$. The most important examples are the following subgroups of "level $N$":

$$\Gamma_0(N) = \left\{ \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \mathrm{SL}_2(\mathbb{Z}) \mid \begin{pmatrix} a & b \\ c & d \end{pmatrix} \equiv \begin{pmatrix} * & * \\ 0 & * \end{pmatrix} \pmod{N} \right\},$$

$$\Gamma_1(N) = \left\{ \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \mathrm{SL}_2(\mathbb{Z}) \mid \begin{pmatrix} a & b \\ c & d \end{pmatrix} \equiv \begin{pmatrix} 1 & * \\ 0 & 1 \end{pmatrix} \pmod{N} \right\},$$

$$\Gamma(N) = \left\{ \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \mathrm{SL}_2(\mathbb{Z}) \mid \begin{pmatrix} a & b \\ c & d \end{pmatrix} \equiv \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} \pmod{N} \right\}.$$

# Other groups

One may also consider functions that satisfy $f(\frac{a\tau+b}{c\tau+d}) = (c\tau+d)^k f(\tau)$ only for $\begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \Gamma$, where $\Gamma$ is a subgroup of finite index in $\mathrm{SL}_2(\mathbb{Z})$. The most important examples are the following subgroups of "level $N$":

$$\Gamma_0(N) = \left\{ \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \mathrm{SL}_2(\mathbb{Z}) \mid \begin{pmatrix} a & b \\ c & d \end{pmatrix} \equiv \begin{pmatrix} * & * \\ 0 & * \end{pmatrix} \pmod{N} \right\},$$

$$\Gamma_1(N) = \left\{ \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \mathrm{SL}_2(\mathbb{Z}) \mid \begin{pmatrix} a & b \\ c & d \end{pmatrix} \equiv \begin{pmatrix} 1 & * \\ 0 & 1 \end{pmatrix} \pmod{N} \right\},$$

$$\Gamma(N) = \left\{ \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \mathrm{SL}_2(\mathbb{Z}) \mid \begin{pmatrix} a & b \\ c & d \end{pmatrix} \equiv \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} \pmod{N} \right\}.$$

The condition (ii) and the definition of cusp forms need to be changed appropriately.

# Why are modular forms important?

From the above definition it may not be clear why modular forms are natural objects.

# Why are modular forms important?

From the above definition it may not be clear why modular forms are natural objects.

**Fact 1**

There exist many different sources of modular forms, often quite dissimilar in nature.

# Why are modular forms important?

From the above definition it may not be clear why modular forms are natural objects.

**Fact 1**

There exist many different sources of modular forms, often quite dissimilar in nature.

**Fact 2**

The spaces of modular forms are finite-dimensional.

# Why are modular forms important?

From the above definition it may not be clear why modular forms are natural objects.

**Fact 1**

There exist many different sources of modular forms, often quite dissimilar in nature.

**Fact 2**

The spaces of modular forms are finite-dimensional.

Because of this one can often prove identities $a_n = b_n$ between sequences of numbers by observing that their generating series land in the same space of modular forms and then checking finitely many of them.

# Modular forms are everywhere!

Modular forms often appear rather unexpectedly.

# Modular forms are everywhere!

Modular forms often appear rather unexpectedly.

- explicit class field theory for imaginary quadratic fields (Kronecker's Jugendtraum)

# Modular forms are everywhere!

Modular forms often appear rather unexpectedly.

- explicit class field theory for imaginary quadratic fields (Kronecker's Jugendtraum)
- irrationality of $\zeta(3)$ (Apéry)

# Modular forms are everywhere!

Modular forms often appear rather unexpectedly.

- explicit class field theory for imaginary quadratic fields (Kronecker's Jugendtraum)
- irrationality of $\zeta(3)$ (Apéry)
- construction of non-torsion rational points on elliptic curves over $\mathbb{Q}$ (Gross-Zagier)

# Modular forms are everywhere!

Modular forms often appear rather unexpectedly.

- explicit class field theory for imaginary quadratic fields (Kronecker's Jugendtraum)
- irrationality of $\zeta(3)$ (Apéry)
- construction of non-torsion rational points on elliptic curves over $\mathbb{Q}$ (Gross-Zagier)
- algebraic independence of $\pi$ and $e^{\pi}$ (Nesterenko)

# Modular forms are everywhere!

Modular forms often appear rather unexpectedly.

- explicit class field theory for imaginary quadratic fields (Kronecker's Jugendtraum)
- irrationality of $\zeta(3)$ (Apéry)
- construction of non-torsion rational points on elliptic curves over $\mathbb{Q}$ (Gross-Zagier)
- algebraic independence of $\pi$ and $e^{\pi}$ (Nesterenko)
- Fermat's Last Theorem (Wiles)

# Modular forms are everywhere!

Modular forms often appear rather unexpectedly.

- explicit class field theory for imaginary quadratic fields (Kronecker's Jugendtraum)
- irrationality of $\zeta(3)$ (Apéry)
- construction of non-torsion rational points on elliptic curves over $\mathbb{Q}$ (Gross-Zagier)
- algebraic independence of $\pi$ and $e^{\pi}$ (Nesterenko)
- Fermat's Last Theorem (Wiles)
- sphere packing problem in 8 dimensions (Viazovska)

# Examples: Eisenstein series

For all even $k > 2$ the function

$$G_k(\tau) := -\frac{B_k}{2k} + \sum_{n \geq 1} \sigma_{k-1}(n) q^n$$

is a modular form of weight $k$ for $\mathrm{SL}_2(\mathbb{Z})$.

# Examples: Eisenstein series

For all even $k > 2$ the function

$$G_k(\tau) := -\frac{B_k}{2k} + \sum_{n \geq 1} \sigma_{k-1}(n) q^n$$

is a modular form of weight $k$ for $SL_2(\mathbb{Z})$. Here

$$\sigma_s(n) = \sum_{d|n} d^s$$

# Examples: Eisenstein series

For all even $k > 2$ the function

$$G_k(\tau) := -\frac{B_k}{2k} + \sum_{n \geq 1} \sigma_{k-1}(n) q^n$$

is a modular form of weight $k$ for $\mathrm{SL}_2(\mathbb{Z})$. Here

$$\sigma_s(n) = \sum_{d|n} d^s$$

The function $G_2(\tau)$ is not a modular form, but transforms according to

$$G_2\left(\frac{a\tau + b}{c\tau + d}\right) = (c\tau + d)^2 G_2(\tau) - \frac{c(c\tau + d)}{4\pi i}$$

# Examples: Eisenstein series

For all even $k > 2$ the function

$$G_k(\tau) := -\frac{B_k}{2k} + \sum_{n\geq 1} \sigma_{k-1}(n) q^n$$

is a modular form of weight $k$ for $\mathrm{SL}_2(\mathbb{Z})$. Here

$$\sigma_s(n) = \sum_{d|n} d^s$$

The function $G_2(\tau)$ is not a modular form, but transforms according to

$$G_2\left(\frac{a\tau + b}{c\tau + d}\right) = (c\tau + d)^2 G_2(\tau) - \frac{c(c\tau + d)}{4\pi i}$$

It is sometimes more convenient to use a normalization

$$E_k(\tau) := 1 - \frac{2k}{B_k} \sum_{n\geq 1} \sigma_{k-1}(n) q^n$$

# Examples: Eisenstein series

As we will see, the space $M_8(\mathrm{SL}_2(\mathbb{Z}))$ is 1-dimensional, and since $E_4^2$ and $E_8$ both belong to it and have the expansion $1 + O(q)$, we must have $E_4^2 = E_8$.

# Examples: Eisenstein series

As we will see, the space $M_8(\mathrm{SL}_2(\mathbb{Z}))$ is 1-dimensional, and since $E_4^2$ and $E_8$ both belong to it and have the expansion $1 + O(q)$, we must have $E_4^2 = E_8$.

This leads to a nontrivial identity

$$\frac{\sigma_7(n) - \sigma_3(n)}{120} = \sum_{m=1}^{n-1} \sigma_3(m)\sigma_3(n-m)$$

# Examples: Eisenstein series

As we will see, the space $M_8(\mathrm{SL}_2(\mathbb{Z}))$ is 1-dimensional, and since $E_4^2$ and $E_8$ both belong to it and have the expansion $1 + O(q)$, we must have $E_4^2 = E_8$.

This leads to a nontrivial identity

$$\frac{\sigma_7(n) - \sigma_3(n)}{120} = \sum_{m=1}^{n-1} \sigma_3(m)\sigma_3(n-m)$$

Simiarly, $E_4 E_6 = E_{10}$, and thus

$$\frac{11\sigma_9(n) - 21\sigma_5(n) + 10\sigma_3(n)}{5040} = \sum_{m=1}^{n-1} \sigma_5(m)\sigma_3(n-m)$$

# Examples: eta-quotients

The Dedekind eta-function

$$\eta(\tau) = q^{\frac{1}{24}} \prod_{n=1}^{\infty}(1 - q^n)$$

satisfies

$$\eta(\tau + 1) = e^{\pi i/12}\eta(\tau)\,, \qquad \eta(-1/\tau) = \sqrt{\tau/i}\,\eta(\tau)$$

# Examples: eta-quotients

The Dedekind eta-function

$$\eta(\tau) = q^{\frac{1}{24}} \prod_{n=1}^{\infty} (1 - q^n)$$

satisfies

$$\eta(\tau + 1) = e^{\pi i/12} \eta(\tau), \qquad \eta(-1/\tau) = \sqrt{\tau/i}\, \eta(\tau)$$

As a corollary,

$$\Delta(\tau) := \eta(\tau)^{24} = q - 24q^2 + 252q^3 + \cdots - 6048q^6 + \ldots$$

is a cusp form of weight 12 for $SL_2(\mathbb{Z})$.

# Examples: eta-quotients

There are many other examples of modular forms that can be written as eta quotients:

$$\frac{\eta^{16}(2\tau)}{\eta^{8}(\tau)} = q + 8q^2 + 28q^3 + 64q^4 + \cdots \in M_4(\Gamma_0(2))$$

$$\eta^4(\tau)\eta^4(5\tau) = q - 4q^2 + 2q^3 + 8q^4 + \cdots \in S_4(\Gamma_0(5))$$

$$\eta^2(\tau)\eta^2(11\tau) = q - 2q^2 - q^3 + 2q^4 + q^5 + \cdots \in S_2(\Gamma_0(11))$$

# Examples: eta-quotients

There are many other examples of modular forms that can be written as eta quotients:

$$\frac{\eta^{16}(2\tau)}{\eta^{8}(\tau)} = q + 8q^2 + 28q^3 + 64q^4 + \cdots \in M_4(\Gamma_0(2))$$

$$\eta^4(\tau)\eta^4(5\tau) = q - 4q^2 + 2q^3 + 8q^4 + \cdots \in S_4(\Gamma_0(5))$$

$$\eta^2(\tau)\eta^2(11\tau) = q - 2q^2 - q^3 + 2q^4 + q^5 + \cdots \in S_2(\Gamma_0(11))$$

One can show that $M_4(\Gamma_0(2))$ is 2-dimensional, and thus

$$\frac{\eta^{16}(2\tau)}{\eta^{8}(\tau)} = G_4(\tau) - G_4(2\tau)$$

# Examples: theta series

Let $\theta(\tau)$ be the Jacobi theta series

$$\theta(\tau) = \sum_{n\in\mathbb{Z}} q^{n^2} = 1 + 2q + 2q^4 + \dots .$$

One can show that $\theta^4(\tau)$ is a modular form of weight 2 for $\Gamma_0(4)$, and since $M_2(\Gamma_0(4))$ is spanned by $G_2(\tau) - 2G_2(2\tau)$ and $G_2(\tau) - 4G_2(4\tau)$, one gets

$$\theta^4(\tau) = 8(G_2(\tau) - 4G_2(4\tau))$$

From this one obtains Jacobi's identity

$$r_4(n) = 8 \sum_{4\nmid d|n,} d\,, \quad n \geq 1\,.$$

This also implies Lagrange's four-square theorem.

# Examples: theta series

If $\Lambda \subset \mathbb{R}^d$ is an even unimodular lattice, then one can show that

$$\Theta_\Lambda(\tau) = \sum_{v \in \Lambda} q^{|v|^2/2}$$

is a modular form of weight $d/2$ for $\mathrm{SL}_2(\mathbb{Z})$.

# Examples: theta series

If $\Lambda \subset \mathbb{R}^d$ is an even unimodular lattice, then one can show that

$$\Theta_\Lambda(\tau) = \sum_{v \in \Lambda} q^{|v|^2/2}$$

is a modular form of weight $d/2$ for $\mathrm{SL}_2(\mathbb{Z})$.

In particular, since the $E_8$-lattice

$$\Lambda_8 = \{(x_1, \ldots, x_8) \in \mathbb{Z}^8 \cup (1/2 + \mathbb{Z})^8 \mid x_1 + \cdots + x_8 = 0 \pmod 2\}$$

is even and unimodular, we have $\Theta_{\Lambda_8}(\tau) \in M_4(\mathrm{SL}_2(\mathbb{Z}))$, and thus one has

$$\Theta_{\Lambda_8}(\tau) = E_4(\tau)$$

# Examples: Euler's pentagonal number theorem

The first example of a nontrivial identity between modular forms was observed by Euler:

$$\prod_{n\geq 1}(1-q^n) = \sum_{n\in\mathbb{Z}}(-1)^n q^{(3n^2-n)/2}\,.$$

# Examples: Euler's pentagonal number theorem

The first example of a nontrivial identity between modular forms was observed by Euler:

$$\prod_{n\geq 1}(1-q^n) = \sum_{n\in\mathbb{Z}}(-1)^n q^{(3n^2-n)/2}\,.$$

To see why this an identity between modular forms, one needs to "complete squares"

$$\frac{3n^2-n}{2} = \frac{(6n-1)^2}{24} - \frac{1}{24}\,,$$

to get an equivalent formulation

$$q^{1/24}\prod_{n\geq 1}(1-q^n) = \sum_{n\in\mathbb{Z}}\chi_{12}(n)q^{n^2/24}\,,$$

where $\chi_{12}\colon \mathbb{Z}\to\{-1,0,1\}$ is a 12-periodic function defined by

$$\chi_{12}(\pm 1) = 1\,,\quad \chi_{12}(\pm 5) = -1\,.$$

# Examples: arithmetic sources

A much deeper source of modular forms is arithmetic geometry. In these examples the coefficients $a_{p^k}$ are obtained by counting the solutions of systems of polynomial equations in finite fields $\mathbb{F}_{p^k}$.

Here is an explicit example. If we denote by $a_n$ the $n$-th Fourier coefficient of

$$f(\tau) = \eta^2(\tau)\eta^2(11\tau) = q - 2q^2 - q^3 + 2q^4 + q^5 + 2q^6 - 2q^7 + \dots ,$$

then

$$a_p = p - \#\{(x, y) \in \mathbb{F}_p^2 \colon y^2 + y = x^3 - x^2\} .$$

# Examples: arithmetic sources

A much deeper source of modular forms is arithmetic geometry. In these examples the coefficients $a_{p^k}$ are obtained by counting the solutions of systems of polynomial equations in finite fields $\mathbb{F}_{p^k}$.
Here is an explicit example. If we denote by $a_n$ the $n$-th Fourier coefficient of

$$f(\tau) = \eta^2(\tau)\eta^2(11\tau) = q - 2q^2 - q^3 + 2q^4 + q^5 + 2q^6 - 2q^7 + \dots ,$$

then

$$a_p = p - \#\{(x, y) \in \mathbb{F}_p^2 \colon y^2 + y = x^3 - x^2\} .$$

This is a special case of the modularity theorem for elliptic curves (in this case for a curve of conductor 11).

# Examples: toric modular forms

There is a construction of modular forms associated to toric varieties due to Borisov and Gunnels. The simplest nontrivial example is

$$T_k(\tau) = \sum_{n_1+\cdots+n_{2k+1}=0} \frac{1}{(1+q^{n_1})\dots(1+q^{n_{2k+1}})} \in M_{2k}(\Gamma_0(2))$$

# Examples: toric modular forms

There is a construction of modular forms associated to toric varieties due to Borisov and Gunnels. The simplest nontrivial example is

$$T_k(\tau) = \sum_{n_1+\cdots+n_{2k+1}=0} \frac{1}{(1+q^{n_1})\dots(1+q^{n_{2k+1}})} \in M_{2k}(\Gamma_0(2))$$

In particular, since $M_2(\Gamma_0(2))$ is 1-dimensional,

$$\sum_{a+b+c=0} \frac{8}{(1+q^a)(1+q^b)(1+q^c)} = E_2(\tau) - 2E_2(2\tau)$$

# Gauss's discovery of modular forms

Gauss was led to consider theta functions when he was studying the arithmetic-geometric mean $M(a, b)$. Let $a \geq b$ be two positive numbers, and define recursively $a_0 = a$, $b_0 = b$, and

$$a_{n+1} = \frac{a_n + b_n}{2}\,, \quad b_{n+1} = \sqrt{a_n b_n}\,, \quad n \geq 0$$

The limit of $a_n$ (or $b_n$) as $n \to \infty$ is the arithmetic-geometric mean $M(a, b)$. Sometime around 1794 he discovered the following remarkable fact. If we denote

$$P(q) = \sum_{n\in\mathbb{Z}} q^{n^2}\,, \qquad Q(q) = \sum_{n\in\mathbb{Z}} (-1)^n q^{n^2}\,,$$

then

$$M(P^2(q), Q^2(q)) = 1\,, \qquad |q| < 1\,.$$

## Gauss's discovery of modular forms

Gauss's proof is based on the following identities

$$P^2(q^2) = \frac{P^2(q) + Q^2(Q)}{2}\,,$$
$$Q^2(q^2) = P(q)Q(q)\,.$$

The first identity is not hard to prove directly, but for the second one essentially needs

$$P(q) = \prod_{n\geq 1}(1-q^{2n})(1+q^{2n-1})^2\,, \qquad Q(q) = \prod_{n\geq 1}(1-q^{2n})(1-q^{2n-1})^2$$

which is equivalent to showing that

$$P(q) = \frac{\eta^5(2\tau)}{\eta^2(\tau)\eta^2(4\tau)}\,, \qquad Q(q) = \frac{\eta^2(\tau)}{\eta(2\tau)}$$