# An introduction to modular forms

Brooks Roberts

University of Idaho

February 22, 2024

# Abstract

In this talk we will motivate the definition of modular forms by considering an interesting example from number theory. Besides presenting the definition, we will also describe the connection between modular forms and the representation theory of GL(2). As a final enticement, we will mention the astonishing connection, via string theory, between certain modular functions and the representation theory of sporadic finite simple groups.

# The Fibonacci sequence

The Fibonacci sequence is the sequence

$$
\begin{aligned}
a(0) &= 0, \\
a(1) &= 1, \\
a(2) &= 1, \\
a(3) &= 2, \\
a(4) &= 3, \\
&\vdots \\
a(n) &= a(n-1) + a(n-2), \qquad n \geq 2.
\end{aligned}
$$

Mathematicians are fascinated by this sequence, and it even has a journal, called the *Fibonacci Quarterly*, that was founded in 1963.

Here is a natural problem: Obtain a formula for $a(n)$.

# The Fibonacci sequence

The Fibonacci sequence is the sequence

$$
\begin{aligned}
a(0) &= 0, \\
a(1) &= 1, \\
a(2) &= 1, \\
a(3) &= 2, \\
a(4) &= 3, \\
&\vdots \\
a(n) &= a(n-1) + a(n-2), \qquad n \geq 2.
\end{aligned}
$$

Mathematicians are fascinated by this sequence, and it even has a journal, called the *Fibonacci Quarterly*, that was founded in 1963.

Here is a natural problem: Obtain a formula for $a(n)$.

# A generating function approach

We can solve this problem by using a generating function.

Let $q$ be a formal variable, and define a formal power series

$$G(q) = a(0) + a(1)q + a(2)q^2 + \cdots,$$

the **generating function** of the sequence $a(n)$.

How does this yield a formula for $a(n)$?

We use $a(n) = a(n-1) + a(n-2)$ to see that

$$G(q) - qG(q) - q^2 G(q) = q.$$

We now solve this for $G(q)$:

# A generating function approach

We can solve this problem by using a generating function.

Let $q$ be a formal variable, and define a formal power series

$$G(q) = a(0) + a(1)q + a(2)q^2 + \cdots,$$

the **generating function** of the sequence $a(n)$.

How does this yield a formula for $a(n)$?

We use $a(n) = a(n-1) + a(n-2)$ to see that

$$G(q) - qG(q) - q^2 G(q) = q.$$

We now solve this for $G(q)$:

# A generating function approach

We can solve this problem by using a generating function.

Let $q$ be a formal variable, and define a formal power series

$$G(q) = a(0) + a(1)q + a(2)q^2 + \cdots,$$

the **generating function** of the sequence $a(n)$.

How does this yield a formula for $a(n)$?

We use $a(n) = a(n-1) + a(n-2)$ to see that

$$G(q) - qG(q) - q^2 G(q) = q.$$

We now solve this for $G(q)$:

# A generating function approach

We can solve this problem by using a generating function.

Let $q$ be a formal variable, and define a formal power series

$$G(q) = a(0) + a(1)q + a(2)q^2 + \cdots,$$

the **generating function** of the sequence $a(n)$.

How does this yield a formula for $a(n)$?

We use $a(n) = a(n-1) + a(n-2)$ to see that

$$G(q) - qG(q) - q^2 G(q) = q.$$

We now solve this for $G(q)$:

# A generating function approach

We can solve this problem by using a generating function.

Let $q$ be a formal variable, and define a formal power series

$$G(q) = a(0) + a(1)q + a(2)q^2 + \cdots,$$

the **generating function** of the sequence $a(n)$.

How does this yield a formula for $a(n)$?

We use $a(n) = a(n-1) + a(n-2)$ to see that

$$G(q) - qG(q) - q^2 G(q) = q.$$

We now solve this for $G(q)$:

# A generating function approach, continued

$$G(q) = \frac{q}{1-q-q^2}$$

$$= \frac{1}{\sqrt{5}} \left( \frac{1}{1 - \frac{1+\sqrt{5}}{2} q} - \frac{1}{1 - \frac{1-\sqrt{5}}{2} q} \right).$$

Next, we recall that there is a formal power series identity:

$$\frac{1}{1-aq} = 1 + aq + a^2 q^2 + \cdots .$$

Using this, we obtain a formula for $a(n)$:

# A generating function approach, continued

$$G(q) = \frac{q}{1-q-q^2}$$
$$= \frac{1}{\sqrt{5}}\left(\frac{1}{1-\frac{1+\sqrt{5}}{2}q} - \frac{1}{1-\frac{1-\sqrt{5}}{2}q}\right).$$

Next, we recall that there is a formal power series identity:

$$\frac{1}{1-aq} = 1 + aq + a^2q^2 + \cdots.$$

Using this, we obtain a formula for $a(n)$:

# A generating function approach, continued

$$G(q) = \frac{q}{1-q-q^2}$$
$$= \frac{1}{\sqrt{5}}\left(\frac{1}{1-\frac{1+\sqrt{5}}{2}q} - \frac{1}{1-\frac{1-\sqrt{5}}{2}q}\right).$$

Next, we recall that there is a formal power series identity:

$$\frac{1}{1-aq} = 1 + aq + a^2q^2 + \cdots.$$

Using this, we obtain a formula for $a(n)$:

# A generating function approach, continued

$$a(n) = \frac{1}{\sqrt{5}} \left( \left( \frac{1+\sqrt{5}}{2} \right)^n - \left( \frac{1-\sqrt{5}}{2} \right)^n \right).$$

This is a nice solution!

So what did we do? We:

- identified an interesting sequence of integers;
- formed the associated generating function;
- noted that the generating function satisfied an equation;
- and finally solved for the generating function, thus obtaining $a(n)$.

# A generating function approach, continued

$$a(n) = \frac{1}{\sqrt{5}} \left( \left( \frac{1+\sqrt{5}}{2} \right)^n - \left( \frac{1-\sqrt{5}}{2} \right)^n \right).$$

This is a nice solution!

So what did we do? We:

- identified an interesting sequence of integers;
- formed the associated generating function;
- noted that the generating function satisfied an equation;
- and finally solved for the generating function, thus obtaining $a(n)$.

# A generating function approach, continued

$$a(n) = \frac{1}{\sqrt{5}} \left( \left( \frac{1+\sqrt{5}}{2} \right)^n - \left( \frac{1-\sqrt{5}}{2} \right)^n \right).$$

This is a nice solution!

So what did we do? We:

- identified an interesting sequence of integers;
- formed the associated generating function;
- noted that the generating function satisfied an equation;
- and finally solved for the generating function, thus obtaining $a(n)$.

# A generating function approach, continued

$$a(n) = \frac{1}{\sqrt{5}} \left( \left( \frac{1+\sqrt{5}}{2} \right)^n - \left( \frac{1-\sqrt{5}}{2} \right)^n \right).$$

This is a nice solution!

So what did we do? We:

- identified an interesting sequence of integers;
- formed the associated generating function;
- noted that the generating function satisfied an equation;
- and finally solved for the generating function, thus obtaining $a(n)$.

# A generating function approach, continued

$$a(n) = \frac{1}{\sqrt{5}} \left( \left( \frac{1+\sqrt{5}}{2} \right)^n - \left( \frac{1-\sqrt{5}}{2} \right)^n \right).$$

This is a nice solution!

So what did we do? We:

- identified an interesting sequence of integers;
- formed the associated generating function;
- noted that the generating function satisfied an equation;
- and finally solved for the generating function, thus obtaining $a(n)$.

# A generating function approach, continued

$$a(n) = \frac{1}{\sqrt{5}} \left( \left( \frac{1+\sqrt{5}}{2} \right)^n - \left( \frac{1-\sqrt{5}}{2} \right)^n \right).$$

This is a nice solution!

So what did we do? We:

- identified an interesting sequence of integers;
- formed the associated generating function;
- noted that the generating function satisfied an equation;
- and finally solved for the generating function, thus obtaining $a(n)$.

# Another sequence

We will apply this approach to another sequence of integers.

Our analysis will not be as simple, but we will arrive at the concept of modular forms and make connections to parts of analysis, geometry, and algebra.

What is our sequence?

A basic problem is to say something about solutions of diophantine equations. Suppose that $p(x, y, z, \dots)$ is a polynomial with integer coefficients, and $n$ is an integer.

What can we say about the solutions to

$$p(x, y, z, \dots) = n$$

in the integers? For example, how many integral solutions are there?

# Another sequence

We will apply this approach to another sequence of integers.

Our analysis will not be as simple, but we will arrive at the concept of modular forms and make connections to parts of analysis, geometry, and algebra.

What is our sequence?

A basic problem is to say something about solutions of diophantine equations. Suppose that $p(x, y, z, \dots)$ is a polynomial with integer coefficients, and $n$ is an integer.

What can we say about the solutions to

$$p(x, y, z, \dots) = n$$

in the integers? For example, how many integral solutions are there?

# Another sequence

We will apply this approach to another sequence of integers.

Our analysis will not be as simple, but we will arrive at the concept of modular forms and make connections to parts of analysis, geometry, and algebra.

What is our sequence?

A basic problem is to say something about solutions of diophantine equations. Suppose that $p(x, y, z, \dots)$ is a polynomial with integer coefficients, and $n$ is an integer.

What can we say about the solutions to

$$p(x, y, z, \dots) = n$$

in the integers? For example, how many integral solutions are there?

# Another sequence

We will apply this approach to another sequence of integers.

Our analysis will not be as simple, but we will arrive at the concept of modular forms and make connections to parts of analysis, geometry, and algebra.

What is our sequence?

A basic problem is to say something about solutions of diophantine equations. Suppose that $p(x, y, z, \dots)$ is a polynomial with integer coefficients, and $n$ is an integer.

What can we say about the solutions to

$$p(x, y, z, \dots) = n$$

in the integers? For example, how many integral solutions are there?

# Another sequence

We will apply this approach to another sequence of integers.

Our analysis will not be as simple, but we will arrive at the concept of modular forms and make connections to parts of analysis, geometry, and algebra.

What is our sequence?

A basic problem is to say something about solutions of diophantine equations. Suppose that $p(x, y, z, \dots)$ is a polynomial with integer coefficients, and $n$ is an integer.

What can we say about the solutions to

$$p(x, y, z, \dots) = n$$

in the integers? For example, how many integral solutions are there?

# Some quadratic forms

In this talk we will look at the case of certain quadratic polynomials. Let $Q(x_1, \ldots, x_m)$ be an integral quadratic form:

$$Q(x) = Q(x_1, \ldots, x_m) = \sum_{i,j}^{m} a_{ij} x_i x_j$$

where $A = (a_{ij})$ is a symmetric matrix with integer coefficients. A simple example is

$$Q(x_1, \ldots, x_m) = x_1^2 + \cdots + x_m^2, \qquad A = \begin{bmatrix} 1 & & \\ & \ddots & \\ & & 1 \end{bmatrix}.$$

So our question would be: in how many ways can an integer be written as a sum of $m$ squares?

# Some quadratic forms

In this talk we will look at the case of certain quadratic polynomials. Let $Q(x_1, \ldots, x_m)$ be an integral quadratic form:

$$Q(x) = Q(x_1, \ldots, x_m) = \sum_{i,j}^{m} a_{ij} x_i x_j$$

where $A = (a_{ij})$ is a symmetric matrix with integer coefficients. A simple example is

$$Q(x_1, \ldots, x_m) = x_1^2 + \cdots + x_m^2, \qquad A = \begin{bmatrix} 1 & & \\ & \ddots & \\ & & 1 \end{bmatrix}.$$

So our question would be: in how many ways can an integer be written as a sum of $m$ squares?

# Some special quadratic forms

To make the exposition simpler, we'll actually consider a different family of examples. We'll assume that

- $Q(x)$ is **positive definite**, i.e., $Q(x) > 0$ for real non-zero $x$;
- $Q(x)$ is **unimodular**, i.e., $\det(A) = 1$;
- $Q(x)$ is **even** for integral $x$.

The last condition is equivalent to the diagonal entries of $A$ being even.

Thus the sum of squares example is not covered.

However, our $Q(x)$ are very interesting.

# Some special quadratic forms

To make the exposition simpler, we'll actually consider a different family of examples. We'll assume that

- $Q(x)$ is **positive definite**, i.e., $Q(x) > 0$ for real non-zero $x$;
- $Q(x)$ is **unimodular**, i.e., $\det(A) = 1$;
- $Q(x)$ is **even** for integral $x$.

The last condition is equivalent to the diagonal entries of $A$ being even.

Thus the sum of squares example is not covered.

However, our $Q(x)$ are very interesting.

# Some special quadratic forms

To make the exposition simpler, we'll actually consider a different family of examples. We'll assume that

- $Q(x)$ is **positive definite**, i.e., $Q(x) > 0$ for real non-zero $x$;
- $Q(x)$ is **unimodular**, i.e., $\det(A) = 1$;
- $Q(x)$ is **even** for integral $x$.

The last condition is equivalent to the diagonal entries of $A$ being even.

Thus the sum of squares example is not covered.

However, our $Q(x)$ are very interesting.

# Some special quadratic forms

To make the exposition simpler, we'll actually consider a different family of examples. We'll assume that

- $Q(x)$ is **positive definite**, i.e., $Q(x) > 0$ for real non-zero $x$;
- $Q(x)$ is **unimodular**, i.e., $\det(A) = 1$;
- $Q(x)$ is **even** for integral $x$.

The last condition is equivalent to the diagonal entries of $A$ being even.

Thus the sum of squares example is not covered.

However, our $Q(x)$ are very interesting.

# Some special quadratic forms

To make the exposition simpler, we'll actually consider a different family of examples. We'll assume that

- $Q(x)$ is **positive definite**, i.e., $Q(x) > 0$ for real non-zero $x$;
- $Q(x)$ is **unimodular**, i.e., $\det(A) = 1$;
- $Q(x)$ is **even** for integral $x$.

The last condition is equivalent to the diagonal entries of $A$ being even.

Thus the sum of squares example is not covered.

However, our $Q(x)$ are very interesting.

# Some special quadratic forms

To make the exposition simpler, we'll actually consider a different family of examples. We'll assume that

- $Q(x)$ is **positive definite**, i.e., $Q(x) > 0$ for real non-zero $x$;
- $Q(x)$ is **unimodular**, i.e., $\det(A) = 1$;
- $Q(x)$ is **even** for integral $x$.

The last condition is equivalent to the diagonal entries of $A$ being even.

Thus the sum of squares example is not covered.

However, our $Q(x)$ are very interesting.

# Our family of quadratic forms

It turns out that such $Q(x)$ are somewhat rare and special (and often related to famous codes).

For example, a necessary condition is that 8 divides $m$.

Moreover, the number of such $Q(x)$ is finite for each $m$:

| $m$ | Number of $Q(x)$ (up to equivalence) |
|---|---|
| 8 | 1 |
| 16 | 2 |
| 24 | 24 |
| 32 | $>$ 80 million |

Let's look at an example.

# Our family of quadratic forms

It turns out that such $Q(x)$ are somewhat rare and special (and often related to famous codes).

For example, a necessary condition is that 8 divides $m$.

Moreover, the number of such $Q(x)$ is finite for each $m$:

| $m$ | Number of $Q(x)$ (up to equivalence) |
|---|---|
| 8 | 1 |
| 16 | 2 |
| 24 | 24 |
| 32 | $>$ 80 million |

Let's look at an example.

# Our family of quadratic forms

It turns out that such $Q(x)$ are somewhat rare and special (and often related to famous codes).

For example, a necessary condition is that 8 divides $m$.

Moreover, the number of such $Q(x)$ is finite for each $m$:

| $m$ | Number of $Q(x)$ (up to equivalence) |
|---|---|
| 8 | 1 |
| 16 | 2 |
| 24 | 24 |
| 32 | $>$ 80 million |

Let's look at an example.

# Our family of quadratic forms

It turns out that such $Q(x)$ are somewhat rare and special (and often related to famous codes).

For example, a necessary condition is that 8 divides $m$.

Moreover, the number of such $Q(x)$ is finite for each $m$:

| $m$ | Number of $Q(x)$ (up to equivalence) |
|---|---|
| 8 | 1 |
| 16 | 2 |
| 24 | 24 |
| 32 | $>$ 80 million |

Let's look at an example.

# The case $m = 8$

The single $Q(x)$ for $m = 8$ corresponds to the 8-dimensional lattice $E_8$.

The $E_8$ lattice is

$$\{(a_1, \ldots, a_8) : \text{all } a_i \in \mathbb{Z} \text{ or all } a_i \in \mathbb{Z} + \frac{1}{2}, \sum_{i=1}^{8} a_i \equiv 0 \pmod 2\}.$$

A basis for this lattice is:

$$e_1 = (2, 0, 0, 0, 0, 0, 0, 0), \qquad e_5 = (0, 0, 0, -1, 1, 0, 0, 0),$$
$$e_2 = (-1, 1, 0, 0, 0, 0, 0, 0), \qquad e_6 = (0, 0, 0, 0, -1, 1, 0, 0),$$
$$e_3 = (0, -1, 1, 0, 0, 0, 0, 0), \qquad e_7 = (0, 0, 0, 0, 0, -1, 1, 0),$$
$$e_4 = (0, 0, -1, 1, 0, 0, 0, 0), \qquad e_8 = (\frac{1}{2}, \frac{1}{2}, \frac{1}{2}, \frac{1}{2}, \frac{1}{2}, \frac{1}{2}, \frac{1}{2}, \frac{1}{2}).$$

# The case $m = 8$, continued

The associated **Gram matrix** of dot products $e_i \cdot e_j$ is

$$A = \begin{bmatrix} 4 & -2 & & & & & & 1 \\ -2 & 2 & -1 & & & & & \\ & -1 & 2 & -1 & & & & \\ & & -1 & 2 & -1 & & & \\ & & & -1 & 2 & -1 & & \\ & & & & -1 & 2 & -1 & \\ & & & & & -1 & 2 & \\ 1 & & & & & & & 2 \end{bmatrix},$$

and our quadratic form is then

$$\begin{aligned} Q(x) = {} & 2(2x_1^2 + x_2^2 + x_3^2 + x_4^2 + x_5^2 + x_6^2 + x_7^2 + x_8^2) \\ & - 2(2x_1x_2 + x_2x_3 + x_3x_4 + x_4x_5 + x_5x_6 + x_6x_7 + x_1x_8). \end{aligned}$$

# The case $m = 8$, continued

For this $A$ it's clear that $Q(x)$ is even for integral $x$, and a calculation shows that $\det(A) = 1$.

But why is it positive definite?

This is because $A$ came from a lattice.

But there is also a convenient criteria:

Let $A(k)$ be the submatrix of $A$ made of the first $k$ rows and columns.

Then $Q(x)$ is positive definite if and only if $\det(A(k)) > 0$ for $k = 1, \ldots, 8$.

In fact,

$$\det(A) = 1, \qquad \det(A(k)) = 4, \quad 1 \leq 1 \leq 7.$$

Thus, $Q(x)$ is positive definite.

# The case $m = 8$, continued

For this $A$ it's clear that $Q(x)$ is even for integral $x$, and a calculation shows that $\det(A) = 1$.

But why is it positive definite?

This is because $A$ came from a lattice.

But there is also a convenient criteria:

Let $A(k)$ be the submatrix of $A$ made of the first $k$ rows and columns.

Then $Q(x)$ is positive definite if and only if $\det(A(k)) > 0$ for $k = 1, \ldots, 8$.

In fact,

$$\det(A) = 1, \qquad \det(A(k)) = 4, \quad 1 \leq 1 \leq 7.$$

Thus, $Q(x)$ is positive definite.

# The case $m = 8$, continued

For this $A$ it's clear that $Q(x)$ is even for integral $x$, and a calculation shows that $\det(A) = 1$.

But why is it positive definite?

This is because $A$ came from a lattice.

But there is also a convenient criteria:

Let $A(k)$ be the submatrix of $A$ made of the first $k$ rows and columns.

Then $Q(x)$ is positive definite if and only if $\det(A(k)) > 0$ for $k = 1, \ldots, 8$.

In fact,

$$\det(A) = 1, \qquad \det(A(k)) = 4, \quad 1 \leq 1 \leq 7.$$

Thus, $Q(x)$ is positive definite.

# The case $m = 8$, continued

For this $A$ it's clear that $Q(x)$ is even for integral $x$, and a calculation shows that $\det(A) = 1$.

But why is it positive definite?

This is because $A$ came from a lattice.

But there is also a convenient criteria:

Let $A(k)$ be the submatrix of $A$ made of the first $k$ rows and columns.

Then $Q(x)$ is positive definite if and only if $\det(A(k)) > 0$ for $k = 1, \ldots, 8$.

In fact,

$$\det(A) = 1, \qquad \det(A(k)) = 4, \quad 1 \leq 1 \leq 7.$$

Thus, $Q(x)$ is positive definite.

# The case $m = 8$, continued

For this $A$ it's clear that $Q(x)$ is even for integral $x$, and a calculation shows that $\det(A) = 1$.

But why is it positive definite?

This is because $A$ came from a lattice.

But there is also a convenient criteria:

Let $A(k)$ be the submatrix of $A$ made of the first $k$ rows and columns.

Then $Q(x)$ is positive definite if and only if $\det(A(k)) > 0$ for $k = 1, \ldots, 8$.

In fact,

$$\det(A) = 1, \qquad \det(A(k)) = 4, \quad 1 \leq 1 \leq 7.$$

Thus, $Q(x)$ is positive definite.

# The case $m = 8$, continued

For this $A$ it's clear that $Q(x)$ is even for integral $x$, and a calculation shows that $\det(A) = 1$.

But why is it positive definite?

This is because $A$ came from a lattice.

But there is also a convenient criteria:

Let $A(k)$ be the submatrix of $A$ made of the first $k$ rows and columns.

Then $Q(x)$ is positive definite if and only if $\det(A(k)) > 0$ for $k = 1, \ldots, 8$.

In fact,

$$\det(A) = 1, \qquad \det(A(k)) = 4, \quad 1 \leq 1 \leq 7.$$

Thus, $Q(x)$ is positive definite.

# The case $m = 16$

When $m = 16$ there are two $Q(x)$ (up to equivalence).

One is $E_8 \oplus E_8$.

The other 16-dimensional $Q(x)$ is called $D_{16}^+$.

It has a definition similar to that of $E_8$.

To learn more about such $Q(x)$, consult the famous book by

**J. H. Conway and N. J. A. Sloane**

called

**Sphere Packings, Lattices and Groups** (3rd edition)

and published by Springer in 1999.

# Back to our problem

Given an integer $n$, we want to say something about the number of integral solutions to $Q(x) = n$.

Given our assumptions, if $n < 0$ or $n$ is odd, then there are no solutions.

So for non-negative integers $n$ we let

$$a(n) = \text{number of integral solutions } x \text{ to } Q(x) = 2n.$$

We are going to calculate the sequence

$$a(0), \quad a(1), \quad a(2), \quad \ldots$$

for $m = 8$ and $m = 16$.

Evidently, we have

$$a(0) = 1.$$

# Back to our problem

Given an integer $n$, we want to say something about the number of integral solutions to $Q(x) = n$.

Given our assumptions, if $n < 0$ or $n$ is odd, then there are no solutions.

So for non-negative integers $n$ we let

$$a(n) = \text{number of integral solutions } x \text{ to } Q(x) = 2n.$$

We are going to calculate the sequence

$$a(0), \quad a(1), \quad a(2), \quad \ldots$$

for $m = 8$ and $m = 16$.

Evidently, we have

$$a(0) = 1.$$

# Back to our problem

Given an integer $n$, we want to say something about the number of integral solutions to $Q(x) = n$.

Given our assumptions, if $n < 0$ or $n$ is odd, then there are no solutions.

So for non-negative integers $n$ we let

$$a(n) = \text{number of integral solutions } x \text{ to } Q(x) = 2n.$$

We are going to calculate the sequence

$$a(0), \quad a(1), \quad a(2), \quad \ldots$$

for $m = 8$ and $m = 16$.

Evidently, we have

$$a(0) = 1.$$

# Back to our problem

Given an integer $n$, we want to say something about the number of integral solutions to $Q(x) = n$.

Given our assumptions, if $n < 0$ or $n$ is odd, then there are no solutions.

So for non-negative integers $n$ we let

$$a(n) = \text{number of integral solutions } x \text{ to } Q(x) = 2n.$$

We are going to calculate the sequence

$$a(0), \quad a(1), \quad a(2), \quad \ldots$$

for $m = 8$ and $m = 16$.

Evidently, we have

$$a(0) = 1.$$

# Back to our problem

Given an integer $n$, we want to say something about the number of integral solutions to $Q(x) = n$.

Given our assumptions, if $n < 0$ or $n$ is odd, then there are no solutions.

So for non-negative integers $n$ we let

$$a(n) = \text{number of integral solutions } x \text{ to } Q(x) = 2n.$$

We are going to calculate the sequence

$$a(0), \quad a(1), \quad a(2), \quad \ldots$$

for $m = 8$ and $m = 16$.

Evidently, we have

$$a(0) = 1.$$

# An analytic generating function

Let's define

$$f(q) = a(0) + a(1)q + a(2)q^2 + \cdots$$

where $q$ is a formal variable.

If our sequence satisfied some linear recurrence relation, then we could solve for $a(n)$ as we did for the Fibonacci sequence.

Unfortunately, there is no such obvious recurrence relation.

Can we still use $f(q)$?

Let's explore: if $q$ is a complex variable, when does $f(q)$ converge?

If $q = 1$, then it's not too hard to see that it diverges.

However, we claim that it converges if $|q| < 1$. Why?

# An analytic generating function

Let's define

$$f(q) = a(0) + a(1)q + a(2)q^2 + \cdots$$

where $q$ is a formal variable.

If our sequence satisfied some linear recurrence relation, then we could solve for $a(n)$ as we did for the Fibonacci sequence.

Unfortunately, there is no such obvious recurrence relation.

Can we still use $f(q)$?

Let's explore: if $q$ is a complex variable, when does $f(q)$ converge?

If $q = 1$, then it's not too hard to see that it diverges.

However, we claim that it converges if $|q| < 1$. Why?

# An analytic generating function

Let's define

$$f(q) = a(0) + a(1)q + a(2)q^2 + \cdots$$

where $q$ is a formal variable.

If our sequence satisfied some linear recurrence relation, then we could solve for $a(n)$ as we did for the Fibonacci sequence.

Unfortunately, there is no such obvious recurrence relation.

Can we still use $f(q)$?

Let's explore: if $q$ is a complex variable, when does $f(q)$ converge?

If $q = 1$, then it's not too hard to see that it diverges.

However, we claim that it converges if $|q| < 1$. Why?

# An analytic generating function

Let's define

$$f(q) = a(0) + a(1)q + a(2)q^2 + \cdots$$

where $q$ is a formal variable.

If our sequence satisfied some linear recurrence relation, then we could solve for $a(n)$ as we did for the Fibonacci sequence.

Unfortunately, there is no such obvious recurrence relation.

Can we still use $f(q)$?

Let's explore: if $q$ is a complex variable, when does $f(q)$ converge?

If $q = 1$, then it's not too hard to see that it diverges.

However, we claim that it converges if $|q| < 1$. Why?

# An analytic generating function

Let's define

$$f(q) = a(0) + a(1)q + a(2)q^2 + \cdots$$

where $q$ is a formal variable.

If our sequence satisfied some linear recurrence relation, then we could solve for $a(n)$ as we did for the Fibonacci sequence.

Unfortunately, there is no such obvious recurrence relation.

Can we still use $f(q)$?

Let's explore: if $q$ is a complex variable, when does $f(q)$ converge?

If $q = 1$, then it's not too hard to see that it diverges.

However, we claim that it converges if $|q| < 1$. Why?

# An analytic generating function

Let's define

$$f(q) = a(0) + a(1)q + a(2)q^2 + \cdots$$

where $q$ is a formal variable.

If our sequence satisfied some linear recurrence relation, then we could solve for $a(n)$ as we did for the Fibonacci sequence.

Unfortunately, there is no such obvious recurrence relation.

Can we still use $f(q)$?

Let's explore: if $q$ is a complex variable, when does $f(q)$ converge?

If $q = 1$, then it's not too hard to see that it diverges.

However, we claim that it converges if $|q| < 1$. Why?

# An analytic generating function

Let's define

$$f(q) = a(0) + a(1)q + a(2)q^2 + \cdots$$

where $q$ is a formal variable.

If our sequence satisfied some linear recurrence relation, then we could solve for $a(n)$ as we did for the Fibonacci sequence.

Unfortunately, there is no such obvious recurrence relation.

Can we still use $f(q)$?

Let's explore: if $q$ is a complex variable, when does $f(q)$ converge?

If $q = 1$, then it's not too hard to see that it diverges.

However, we claim that it converges if $|q| < 1$. Why?

# Convergence for $|q| < 1$

Let's begin by noticing the following:

$$f(q) = a(0) + a(1)q + a(2)q^2 + \cdots = \sum_{x \in \mathbb{Z}^m} q^{Q(x)/2}.$$

Consider $Q(x)$. Since $Q(x)$ is positive-definite,

$$\sqrt{Q(x)}$$

is a **norm** on $\mathbb{R}^m$. But all norms on $\mathbb{R}^m$ are equivalent! So for some $c > 0$,

$$Q(x) \geq c(x_1^2 + \cdots + x_m^2), \qquad x \in \mathbb{R}^m.$$

Hence, for $|q| < 1$,

$$\sum_{x \in \mathbb{Z}^m} |q|^{Q(x)/2} \leq \sum_{x \in \mathbb{Z}^m} |q|^{c(x_1^2 + \cdots + x_m^2)/2} \leq \left( \sum_{x \in \mathbb{Z}} |q|^{cx^2/2} \right)^m.$$

# Convergence for $|q| < 1$

Let's begin by noticing the following:

$$f(q) = a(0) + a(1)q + a(2)q^2 + \cdots = \sum_{x \in \mathbb{Z}^m} q^{Q(x)/2}.$$

Consider $Q(x)$. Since $Q(x)$ is positive-definite,

$$\sqrt{Q(x)}$$

is a **norm** on $\mathbb{R}^m$. But all norms on $\mathbb{R}^m$ are equivalent! So for some $c > 0$,

$$Q(x) \geq c(x_1^2 + \cdots + x_m^2), \qquad x \in \mathbb{R}^m.$$

Hence, for $|q| < 1$,

$$\sum_{x \in \mathbb{Z}^m} |q|^{Q(x)/2} \leq \sum_{x \in \mathbb{Z}^m} |q|^{c(x_1^2 + \cdots + x_m^2)/2} \leq \left( \sum_{x \in \mathbb{Z}} |q|^{cx^2/2} \right)^m.$$

# Convergence for $|q| < 1$

Let's begin by noticing the following:

$$f(q) = a(0) + a(1)q + a(2)q^2 + \cdots = \sum_{x \in \mathbb{Z}^m} q^{Q(x)/2}.$$

Consider $Q(x)$. Since $Q(x)$ is positive-definite,

$$\sqrt{Q(x)}$$

is a **norm** on $\mathbb{R}^m$. But all norms on $\mathbb{R}^m$ are equivalent! So for some $c > 0$,

$$Q(x) \geq c(x_1^2 + \cdots + x_m^2), \qquad x \in \mathbb{R}^m.$$

Hence, for $|q| < 1$,

$$\sum_{x \in \mathbb{Z}^m} |q|^{Q(x)/2} \leq \sum_{x \in \mathbb{Z}^m} |q|^{c(x_1^2 + \cdots + x_m^2)/2} \leq \left( \sum_{x \in \mathbb{Z}} |q|^{cx^2/2} \right)^m.$$

# Convergence for $|q| < 1$

Let's begin by noticing the following:

$$f(q) = a(0) + a(1)q + a(2)q^2 + \cdots = \sum_{x \in \mathbb{Z}^m} q^{Q(x)/2}.$$

Consider $Q(x)$. Since $Q(x)$ is positive-definite,

$$\sqrt{Q(x)}$$

is a **norm** on $\mathbb{R}^m$. But all norms on $\mathbb{R}^m$ are equivalent! So for some $c > 0$,

$$Q(x) \geq c(x_1^2 + \cdots + x_m^2), \qquad x \in \mathbb{R}^m.$$

Hence, for $|q| < 1$,

$$\sum_{x \in \mathbb{Z}^m} |q|^{Q(x)/2} \leq \sum_{x \in \mathbb{Z}^m} |q|^{c(x_1^2 + \cdots + x_m^2)/2} \leq \left( \sum_{x \in \mathbb{Z}} |q|^{cx^2/2} \right)^m.$$

# Convergence for $|q| < 1$

Let's begin by noticing the following:

$$f(q) = a(0) + a(1)q + a(2)q^2 + \cdots = \sum_{x \in \mathbb{Z}^m} q^{Q(x)/2}.$$

Consider $Q(x)$. Since $Q(x)$ is positive-definite,

$$\sqrt{Q(x)}$$

is a **norm** on $\mathbb{R}^m$. But all norms on $\mathbb{R}^m$ are equivalent! So for some $c > 0$,

$$Q(x) \geq c(x_1^2 + \cdots + x_m^2), \qquad x \in \mathbb{R}^m.$$

Hence, for $|q| < 1$,

$$\sum_{x \in \mathbb{Z}^m} |q|^{Q(x)/2} \leq \sum_{x \in \mathbb{Z}^m} |q|^{c(x_1^2 + \cdots + x_m^2)/2} \leq \left( \sum_{x \in \mathbb{Z}} |q|^{cx^2/2} \right)^m.$$

# A change of variables

By comparison to the geometric series, $f(q)$ converges for $|q| < 1$. In fact, by the Weierstrass $M$-test, $f(q)$ converges uniformly in closed discs inside $|q| < 1$ to an analytic function.

Next, it's convenient to change variables. We will pre-compose $f(q)$ with

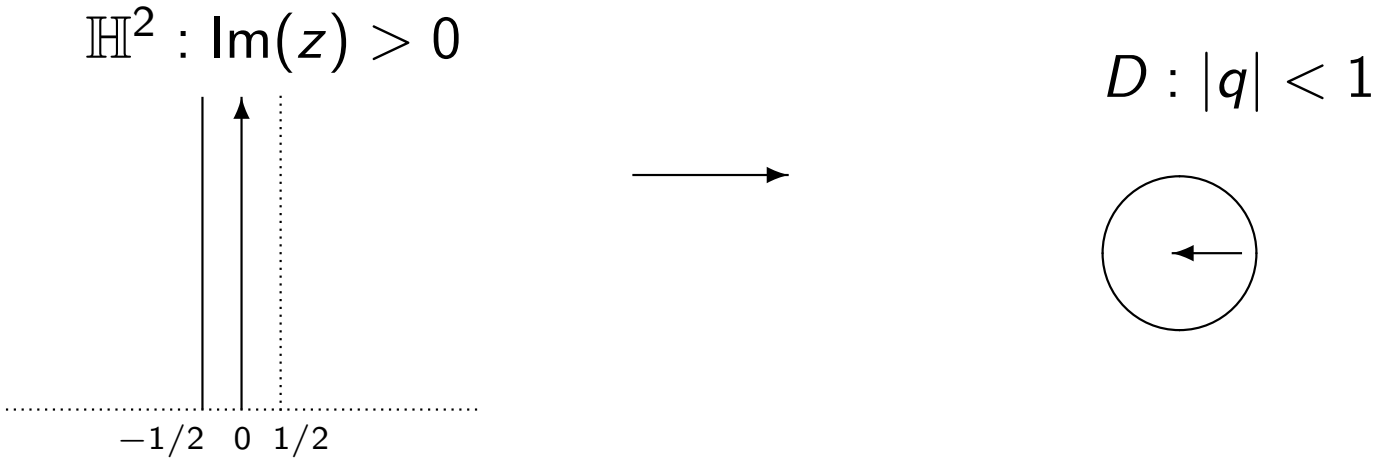
$$\mathbb{H}^2 = \{z \in \mathbb{C} : \mathrm{Im}(z) > 0\} \longrightarrow D = \{q \in \mathbb{C} : |q| < 1\},$$
$$z = x + iy \mapsto q = e^{2\pi i z} = e^{2\pi i x} e^{-2\pi y}.$$

# A change of variables

By comparison to the geometric series, $f(q)$ converges for $|q| < 1$. In fact, by the Weierstrass $M$-test, $f(q)$ converges uniformly in closed discs inside $|q| < 1$ to an analytic function.

Next, it's convenient to change variables. We will pre-compose $f(q)$ with

$$\mathbb{H}^2 = \{z \in \mathbb{C} : \mathrm{Im}(z) > 0\} \longrightarrow D = \{q \in \mathbb{C} : |q| < 1\},$$
$$z = x + iy \mapsto q = e^{2\pi i z} = e^{2\pi i x} e^{-2\pi y}.$$



# A theta series

Note that the change of variables $z \mapsto q$ is

- not onto, as it misses 0;
- not one-to-one, as any two vertical lines which are one unit apart get mapped to the same line in the disc.

We now define

$$\theta(z) = f(q), \qquad z \in \mathbb{H}^2.$$

This function is analytic on the entire upper half plane $\mathbb{H}^2$.

It is an example of a **theta series**, and we are going to study it.

# A theta series

Note that the change of variables $z \mapsto q$ is

- not onto, as it misses 0;
- not one-to-one, as any two vertical lines which are one unit apart get mapped to the same line in the disc.

We now define

$$\theta(z) = f(q), \qquad z \in \mathbb{H}^2.$$

This function is analytic on the entire upper half plane $\mathbb{H}^2$.

It is an example of a **theta series**, and we are going to study it.

# Symmetry properties

The theta series $\theta(z)$ has remarkable symmetry properties.

The first symmetry property is that

$$\theta(z+1) = \theta(z), \qquad z \in \mathbb{H}^2.$$

This is easy:

$$\theta(z+1) = \sum_{x \in \mathbb{Z}^m} e^{2\pi i \frac{Q(x)}{2}(z+1)} = \sum_{x \in \mathbb{Z}^m} e^{2\pi i \frac{Q(x)}{2}} \cdot e^{2\pi i \frac{Q(x)}{2} z} = \theta(z).$$

The second symmetry property is not so obvious. We claim that

$$\theta(-1/z)(-z)^{-m/2} = \theta(z), \qquad z \in \mathbb{H}^2.$$

Note that if $z \in \mathbb{H}^2$, then $-1/z \in \mathbb{H}^2$, so the equation is meaningful.

# Symmetry properties

The theta series $\theta(z)$ has remarkable symmetry properties.

The first symmetry property is that

$$\theta(z+1) = \theta(z), \qquad z \in \mathbb{H}^2.$$

This is easy:

$$\theta(z+1) = \sum_{x \in \mathbb{Z}^m} e^{2\pi i \frac{Q(x)}{2}(z+1)} = \sum_{x \in \mathbb{Z}^m} e^{2\pi i \frac{Q(x)}{2}} \cdot e^{2\pi i \frac{Q(x)}{2} z} = \theta(z).$$

The second symmetry property is not so obvious. We claim that

$$\theta(-1/z)(-z)^{-m/2} = \theta(z), \qquad z \in \mathbb{H}^2.$$

Note that if $z \in \mathbb{H}^2$, then $-1/z \in \mathbb{H}^2$, so the equation is meaningful.

# Symmetry properties

The theta series $\theta(z)$ has remarkable symmetry properties.

The first symmetry property is that

$$\theta(z+1) = \theta(z), \qquad z \in \mathbb{H}^2.$$

This is easy:

$$\theta(z+1) = \sum_{x \in \mathbb{Z}^m} e^{2\pi i \frac{Q(x)}{2}(z+1)} = \sum_{x \in \mathbb{Z}^m} e^{2\pi i \frac{Q(x)}{2}} \cdot e^{2\pi i \frac{Q(x)}{2} z} = \theta(z).$$

The second symmetry property is not so obvious. We claim that

$$\theta(-1/z)(-z)^{-m/2} = \theta(z), \qquad z \in \mathbb{H}^2.$$

Note that if $z \in \mathbb{H}^2$, then $-1/z \in \mathbb{H}^2$, so the equation is meaningful.

# Symmetry properties, continued

How can we prove

$$\theta(-1/z)(-z)^{-m/2} = \theta(z), \qquad z \in \mathbb{H}^2 \ ?$$

Both sides are analytic functions on $\mathbb{H}^2$.

By the Identity Principle, it would suffice to prove this for $z = it$, $t > 0$.

Now for $t > 0$,

$$\theta(it) = \sum_{z \in \mathbb{Z}^m} e^{-\pi t Q(x)} = \sum_{x \in \mathbb{Z}^m} g_t(x)$$

where we define

$$g_t(x) = e^{-\pi t Q(x)}, \qquad x \in \mathbb{R}^m.$$

What we have here is a function on the continuous domain $\mathbb{R}^m$ summed over the discrete lattice $\mathbb{Z}^m$ ... hmmm where have I seen that ...

# Symmetry properties, continued

How can we prove

$$\theta(-1/z)(-z)^{-m/2} = \theta(z), \qquad z \in \mathbb{H}^2 \ ?$$

Both sides are analytic functions on $\mathbb{H}^2$.

By the Identity Principle, it would suffice to prove this for $z = it$, $t > 0$.

Now for $t > 0$,

$$\theta(it) = \sum_{z \in \mathbb{Z}^m} e^{-\pi t Q(x)} = \sum_{x \in \mathbb{Z}^m} g_t(x)$$

where we define

$$g_t(x) = e^{-\pi t Q(x)}, \qquad x \in \mathbb{R}^m.$$

What we have here is a function on the continuous domain $\mathbb{R}^m$ summed over the discrete lattice $\mathbb{Z}^m$ ... hmmm where have I seen that ...

# Symmetry properties, continued

How can we prove

$$\theta(-1/z)(-z)^{-m/2} = \theta(z), \qquad z \in \mathbb{H}^2 \ ?$$

Both sides are analytic functions on $\mathbb{H}^2$.

By the Identity Principle, it would suffice to prove this for $z = it$, $t > 0$.

Now for $t > 0$,

$$\theta(it) = \sum_{z \in \mathbb{Z}^m} e^{-\pi t Q(x)} = \sum_{x \in \mathbb{Z}^m} g_t(x)$$

where we define

$$g_t(x) = e^{-\pi t Q(x)}, \qquad x \in \mathbb{R}^m.$$

What we have here is a function on the continuous domain $\mathbb{R}^m$ summed over the discrete lattice $\mathbb{Z}^m$ ... hmmm where have I seen that ...

# Symmetry properties, continued

How can we prove

$$\theta(-1/z)(-z)^{-m/2} = \theta(z), \qquad z \in \mathbb{H}^2 \ ?$$

Both sides are analytic functions on $\mathbb{H}^2$.

By the Identity Principle, it would suffice to prove this for $z = it$, $t > 0$.

Now for $t > 0$,

$$\theta(it) = \sum_{z \in \mathbb{Z}^m} e^{-\pi t Q(x)} = \sum_{x \in \mathbb{Z}^m} g_t(x)$$

where we define

$$g_t(x) = e^{-\pi t Q(x)}, \qquad x \in \mathbb{R}^m.$$

What we have here is a function on the continuous domain $\mathbb{R}^m$ summed over the discrete lattice $\mathbb{Z}^m$ ... hmmm where have I seen that ...

# Symmetry properties, continued

How can we prove

$$\theta(-1/z)(-z)^{-m/2} = \theta(z), \qquad z \in \mathbb{H}^2 \ ?$$

Both sides are analytic functions on $\mathbb{H}^2$.

By the Identity Principle, it would suffice to prove this for $z = it$, $t > 0$.

Now for $t > 0$,

$$\theta(it) = \sum_{z \in \mathbb{Z}^m} e^{-\pi t Q(x)} = \sum_{x \in \mathbb{Z}^m} g_t(x)$$

where we define

$$g_t(x) = e^{-\pi t Q(x)}, \qquad x \in \mathbb{R}^m.$$

What we have here is a function on the continuous domain $\mathbb{R}^m$ summed over the discrete lattice $\mathbb{Z}^m$ ... hmmm where have I seen that ...

# The Poisson summation formula

In Fourier analysis, and the **Poisson summation formula**.

This formula asserts that

$$\sum_{x \in \mathbb{Z}^m} g(x) = \sum_{x \in \mathbb{Z}^m} \hat{g}(x)$$

for rapidly decaying functions $g$ on $\mathbb{R}^m$, where

$$\hat{g}(x) = \int_{\mathbb{R}^m} g(y) e^{-2\pi i \, x \cdot y} \, dy$$

is the **Fourier transform** of $g(x)$.

($x \cdot y$ is the usual dot product on $\mathbb{R}^m$, as in the definition of $E_8$.)

We are thus reduced to computing the Fourier transform $\hat{g}_t(x)$.

# The Poisson summation formula

In Fourier analysis, and the **Poisson summation formula**.

This formula asserts that

$$\sum_{x \in \mathbb{Z}^m} g(x) = \sum_{x \in \mathbb{Z}^m} \hat{g}(x)$$

for rapidly decaying functions $g$ on $\mathbb{R}^m$, where

$$\hat{g}(x) = \int_{\mathbb{R}^m} g(y) e^{-2\pi i \, x \cdot y} \, dy$$

is the **Fourier transform** of $g(x)$.

($x \cdot y$ is the usual dot product on $\mathbb{R}^m$, as in the definition of $E_8$.)

We are thus reduced to computing the Fourier transform $\hat{g}_t(x)$.

# Completing the argument

To compute $\hat{g}_t(x)$ we:

- write $A = {}^{\mathrm{t}}BB$ for some $B \in \mathrm{M}(m, \mathbb{R})$;
- make some variable changes;
- and then use that the one variable Fourier transform of the **Gaussian** $e^{-\pi x^2}$ is itself, so that

$$\hat{g}_t(x) = \sqrt{t}^{-m} e^{-\pi t^{-1}\, {}^{\mathrm{t}}xA^{-1}x}.$$

Using the Poisson summation formula we then obtain:

$$\theta(it) = (-it)^{-m/2}\theta(-1/it), \qquad t > 0.$$

This proves the second symmetry property

$$\theta(-1/z)(-z)^{-m/2} = \theta(z), \qquad z \in \mathbb{H}^2.$$

# Completing the argument

To compute $\hat{g}_t(x)$ we:

- write $A = {}^{\mathrm{t}}BB$ for some $B \in \mathrm{M}(m, \mathbb{R})$;
- make some variable changes;
- and then use that the one variable Fourier transform of the **Gaussian** $e^{-\pi x^2}$ is itself, so that

$$\hat{g}_t(x) = \sqrt{t}^{-m} e^{-\pi t^{-1}\, {}^{\mathrm{t}}xA^{-1}x}.$$

Using the Poisson summation formula we then obtain:

$$\theta(it) = (-it)^{-m/2}\theta(-1/it), \qquad t > 0.$$

This proves the second symmetry property

$$\theta(-1/z)(-z)^{-m/2} = \theta(z), \qquad z \in \mathbb{H}^2.$$

# What does this mean?

So far we:

- introduced the generating sequence for our sequence;
- showed that it has good analytic properties;
- and proved that it satisfies two functional equations.

But what does this mean, i.e., is there a conceptual interpretation?

For this, we note that the two symmetries

$$z \mapsto z+1, \qquad z \mapsto -1/z$$

in the functional equations are Mobius transformations. If

$$\alpha = \begin{bmatrix} a & b \\ c & d \end{bmatrix} \in \mathrm{SL}(2,\mathbb{R}),\ (\text{i.e., } a,b,c,d \in \mathbb{R},\ \det(\begin{bmatrix} a & b \\ c & d \end{bmatrix}) = 1)$$

# What does this mean?

So far we:

- introduced the generating sequence for our sequence;
- showed that it has good analytic properties;
- and proved that it satisfies two functional equations.

But what does this mean, i.e., is there a conceptual interpretation?

For this, we note that the two symmetries

$$z \mapsto z+1, \qquad z \mapsto -1/z$$

in the functional equations are Mobius transformations. If

$$\alpha = \begin{bmatrix} a & b \\ c & d \end{bmatrix} \in \mathrm{SL}(2,\mathbb{R}),\ (\text{i.e., } a,b,c,d \in \mathbb{R},\ \det(\begin{bmatrix} a & b \\ c & d \end{bmatrix}) = 1)$$

# What does this mean?

So far we:

- introduced the generating sequence for our sequence;
- showed that it has good analytic properties;
- and proved that it satisfies two functional equations.

But what does this mean, i.e., is there a conceptual interpretation?

For this, we note that the two symmetries

$$z \mapsto z+1, \qquad z \mapsto -1/z$$

in the functional equations are Mobius transformations. If

$$\alpha = \begin{bmatrix} a & b \\ c & d \end{bmatrix} \in \mathrm{SL}(2,\mathbb{R}),\ (\text{i.e., } a,b,c,d \in \mathbb{R},\ \det(\begin{bmatrix} a & b \\ c & d \end{bmatrix}) = 1)$$

# What does this mean?

So far we:

- introduced the generating sequence for our sequence;
- showed that it has good analytic properties;
- and proved that it satisfies two functional equations.

But what does this mean, i.e., is there a conceptual interpretation?

For this, we note that the two symmetries

$$z \mapsto z+1, \qquad z \mapsto -1/z$$

in the functional equations are Mobius transformations. If

$$\alpha = \begin{bmatrix} a & b \\ c & d \end{bmatrix} \in \mathrm{SL}(2,\mathbb{R}),\ (\text{i.e., } a,b,c,d \in \mathbb{R},\ \det(\begin{bmatrix} a & b \\ c & d \end{bmatrix}) = 1)$$

# What does this mean?

So far we:

- introduced the generating sequence for our sequence;
- showed that it has good analytic properties;
- and proved that it satisfies two functional equations.

But what does this mean, i.e., is there a conceptual interpretation?

For this, we note that the two symmetries

$$z \mapsto z+1, \qquad z \mapsto -1/z$$

in the functional equations are Mobius transformations. If

$$\alpha = \begin{bmatrix} a & b \\ c & d \end{bmatrix} \in \mathrm{SL}(2,\mathbb{R}),\ (\text{i.e., } a,b,c,d \in \mathbb{R},\ \det(\begin{bmatrix} a & b \\ c & d \end{bmatrix}) = 1)$$

# What does this mean?

So far we:

- introduced the generating sequence for our sequence;
- showed that it has good analytic properties;
- and proved that it satisfies two functional equations.

But what does this mean, i.e., is there a conceptual interpretation?

For this, we note that the two symmetries

$$z \mapsto z+1, \qquad z \mapsto -1/z$$

in the functional equations are Mobius transformations. If

$$\alpha = \begin{bmatrix} a & b \\ c & d \end{bmatrix} \in \mathrm{SL}(2,\mathbb{R}),\ (\text{i.e., } a,b,c,d \in \mathbb{R},\ \det(\begin{bmatrix} a & b \\ c & d \end{bmatrix}) = 1)$$

# What does this mean?

So far we:

- introduced the generating sequence for our sequence;
- showed that it has good analytic properties;
- and proved that it satisfies two functional equations.

But what does this mean, i.e., is there a conceptual interpretation?

For this, we note that the two symmetries

$$z \mapsto z+1, \qquad z \mapsto -1/z$$

in the functional equations are Mobius transformations. If

$$\alpha = \begin{bmatrix} a & b \\ c & d \end{bmatrix} \in \mathrm{SL}(2,\mathbb{R}),\ (\text{i.e., } a,b,c,d \in \mathbb{R},\ \det(\begin{bmatrix} a & b \\ c & d \end{bmatrix}) = 1)$$

# Mobius transformations

then the function

$$z \mapsto \alpha \cdot z = \frac{az + b}{cz + d}$$

defines an automorphism of $\mathbb{H}^2$ because

$$\mathrm{Im}(\alpha \cdot z) = \frac{z}{|cz + d|^2}.$$

The function $z \mapsto \alpha \cdot z$ is called a **Mobius transformation**.

Moreover, for $\alpha, \beta \in \mathrm{SL}(2, \mathbb{R})$,

$$(\alpha\beta) \cdot z = \alpha \cdot (\beta \cdot z), \qquad z \in \mathbb{H}^2.$$

Thus, $\mathrm{SL}(2, \mathbb{R})$ acts on the upper half-plane $\mathbb{H}^2$.

# Mobius transformations

then the function

$$z \mapsto \alpha \cdot z = \frac{az + b}{cz + d}$$

defines an automorphism of $\mathbb{H}^2$ because

$$\mathrm{Im}(\alpha \cdot z) = \frac{z}{|cz + d|^2}.$$

The function $z \mapsto \alpha \cdot z$ is called a **Mobius transformation**.

Moreover, for $\alpha, \beta \in \mathrm{SL}(2, \mathbb{R})$,

$$(\alpha\beta) \cdot z = \alpha \cdot (\beta \cdot z), \qquad z \in \mathbb{H}^2.$$

Thus, $\mathrm{SL}(2, \mathbb{R})$ acts on the upper half-plane $\mathbb{H}^2$.

# The meaning of the functional equations

Now evidently,

$$z+1 = T \cdot z, \qquad -1/z = S \cdot z$$

with

$$T = \begin{bmatrix} 1 & 1 \\ 0 & 1 \end{bmatrix}, \qquad S = \begin{bmatrix} 0 & 1 \\ -1 & 0 \end{bmatrix}.$$

We can thus rewrite the functional equations as

$$\theta(T \cdot z) = \theta(z),$$
$$\theta(S \cdot z)(-z)^{-m/2} = \theta(z)$$

for $z \in \mathbb{H}^2$.

Can we make this even more conceptual?

Let's think about the factor $(-z)^{-m/2}$ in the second functional equation.

# The meaning of the functional equations

Now evidently,

$$z+1 = T\cdot z, \qquad -1/z = S\cdot z$$

with

$$T = \begin{bmatrix} 1 & 1 \\ 0 & 1 \end{bmatrix}, \qquad S = \begin{bmatrix} 0 & 1 \\ -1 & 0 \end{bmatrix}.$$

We can thus rewrite the functional equations as

$$\theta(T\cdot z) = \theta(z),$$
$$\theta(S\cdot z)(-z)^{-m/2} = \theta(z)$$

for $z \in \mathbb{H}^2$.

Can we make this even more conceptual?

Let's think about the factor $(-z)^{-m/2}$ in the second functional equation.

# The meaning of the functional equations

Now evidently,

$$z+1 = T\cdot z, \qquad -1/z = S\cdot z$$

with

$$T = \begin{bmatrix} 1 & 1 \\ 0 & 1 \end{bmatrix}, \qquad S = \begin{bmatrix} 0 & 1 \\ -1 & 0 \end{bmatrix}.$$

We can thus rewrite the functional equations as

$$\theta(T\cdot z) = \theta(z),$$
$$\theta(S\cdot z)(-z)^{-m/2} = \theta(z)$$

for $z \in \mathbb{H}^2$.

Can we make this even more conceptual?

Let's think about the factor $(-z)^{-m/2}$ in the second functional equation.

# The meaning of the functional equations

Now evidently,

$$z+1 = T\cdot z, \qquad -1/z = S\cdot z$$

with

$$T = \begin{bmatrix} 1 & 1 \\ 0 & 1 \end{bmatrix}, \qquad S = \begin{bmatrix} 0 & 1 \\ -1 & 0 \end{bmatrix}.$$

We can thus rewrite the functional equations as

$$\theta(T\cdot z) = \theta(z),$$
$$\theta(S\cdot z)(-z)^{-m/2} = \theta(z)$$

for $z \in \mathbb{H}^2$.

Can we make this even more conceptual?

Let's think about the factor $(-z)^{-m/2}$ in the second functional equation.

# The meaning of the functional equations, continued

Let's (cleverly) define

$$j(\alpha, z) = j(\begin{bmatrix} a & b \\ c & d \end{bmatrix}, z) = cz + d,$$

for $\alpha = \left[\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right] \in \mathrm{SL}(2, \mathbb{R})$ and $z \in \mathbb{H}^2$.

Then the functional equations are now

$$\theta(T \cdot z) j(T, z)^{-m/2} = \theta(z),$$
$$\theta(S \cdot z) j(S, z)^{-m/2} = \theta(z)$$

because

$$j(T, z) = j(\begin{bmatrix} 1 & 1 \\ 0 & 1 \end{bmatrix}, z) = 1, \qquad j(S, z) = j(\begin{bmatrix} 0 & 1 \\ -1 & 0 \end{bmatrix}, z) = -z.$$

# The meaning of the functional equations, continued

Let's (cleverly) define

$$j(\alpha, z) = j(\begin{bmatrix} a & b \\ c & d \end{bmatrix}, z) = cz + d,$$

for $\alpha = \left[\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right] \in \mathrm{SL}(2, \mathbb{R})$ and $z \in \mathbb{H}^2$.

Then the functional equations are now

$$\theta(T \cdot z) j(T, z)^{-m/2} = \theta(z),$$
$$\theta(S \cdot z) j(S, z)^{-m/2} = \theta(z)$$

because

$$j(T, z) = j(\begin{bmatrix} 1 & 1 \\ 0 & 1 \end{bmatrix}, z) = 1, \qquad j(S, z) = j(\begin{bmatrix} 0 & 1 \\ -1 & 0 \end{bmatrix}, z) = -z.$$

# The meaning of the functional equations, continued

Does this rewrite actual do anything?

Yes.

The **automorphy factor** $j$ satisfies the **cocycle condition**

$$j(\alpha\beta, z) = j(\alpha, \beta \cdot z) j(\beta, z), \qquad \alpha, \beta \in \mathrm{SL}(2, \mathbb{R}), \quad z \in \mathbb{H}^2.$$

This suggests we define

$$(f \mid \alpha)(z) = f(\alpha \cdot z) j(\alpha, z)^{-m/2}$$

for $\alpha \in \mathrm{SL}(2, \mathbb{R})$ and $f : \mathbb{H}^2 \to \mathbb{C}$, because then for $\alpha, \beta \in \mathrm{SL}(2, \mathbb{R})$,

$$(f \mid \alpha) \mid \beta = f \mid \alpha\beta,$$

i.e., "slash" $\mid$ is a right action of $\mathrm{SL}(2, \mathbb{R})$ on functions on $\mathbb{H}^2$.

# The meaning of the functional equations, continued

Does this rewrite actual do anything?

Yes.

The **automorphy factor** $j$ satisfies the **cocycle condition**

$$j(\alpha\beta, z) = j(\alpha, \beta \cdot z) j(\beta, z), \qquad \alpha, \beta \in \mathrm{SL}(2, \mathbb{R}), \quad z \in \mathbb{H}^2.$$

This suggests we define

$$(f \mid \alpha)(z) = f(\alpha \cdot z) j(\alpha, z)^{-m/2}$$

for $\alpha \in \mathrm{SL}(2, \mathbb{R})$ and $f : \mathbb{H}^2 \to \mathbb{C}$, because then for $\alpha, \beta \in \mathrm{SL}(2, \mathbb{R})$,

$$(f \mid \alpha) \mid \beta = f \mid \alpha\beta,$$

i.e., "slash" $\mid$ is a right action of $\mathrm{SL}(2, \mathbb{R})$ on functions on $\mathbb{H}^2$.

# The meaning of the functional equations, continued

Does this rewrite actual do anything?

Yes.

The **automorphy factor** $j$ satisfies the **cocycle condition**

$$j(\alpha\beta, z) = j(\alpha, \beta \cdot z) j(\beta, z), \qquad \alpha, \beta \in \mathsf{SL}(2, \mathbb{R}), \quad z \in \mathbb{H}^2.$$

This suggests we define

$$(f \mid \alpha)(z) = f(\alpha \cdot z) j(\alpha, z)^{-m/2}$$

for $\alpha \in \mathsf{SL}(2, \mathbb{R})$ and $f : \mathbb{H}^2 \to \mathbb{C}$, because then for $\alpha, \beta \in \mathsf{SL}(2, \mathbb{R})$,

$$(f \mid \alpha) \mid \beta = f \mid \alpha\beta,$$

i.e., "slash" $\mid$ is a right action of $\mathsf{SL}(2, \mathbb{R})$ on functions on $\mathbb{H}^2$.

# The meaning of the functional equations, continued

Does this rewrite actual do anything?

Yes.

The **automorphy factor** $j$ satisfies the **cocycle condition**

$$j(\alpha\beta, z) = j(\alpha, \beta \cdot z) j(\beta, z), \qquad \alpha, \beta \in \mathrm{SL}(2, \mathbb{R}), \quad z \in \mathbb{H}^2.$$

This suggests we define

$$(f \mid \alpha)(z) = f(\alpha \cdot z) j(\alpha, z)^{-m/2}$$

for $\alpha \in \mathrm{SL}(2, \mathbb{R})$ and $f : \mathbb{H}^2 \to \mathbb{C}$, because then for $\alpha, \beta \in \mathrm{SL}(2, \mathbb{R})$,

$$(f \mid \alpha) \mid \beta = f \mid \alpha\beta,$$

i.e., "slash" $\mid$ is a right action of $\mathrm{SL}(2, \mathbb{R})$ on functions on $\mathbb{H}^2$.

# The meaning of the functional equations, continued

We can now rewrite the functional equations very simply as

$$\theta \mid T = \theta, \qquad \theta \mid S = \theta.$$

Moreover, since "slash" $\mid$ is a right action we can even say that

$$\theta \mid \alpha = \theta$$

for $\alpha$ in the subgroup $\langle T, S \rangle$ of $\mathrm{SL}(2, \mathbb{R})$ generated by $T$ and $S$.

But what is $\langle T, S \rangle$? Can this get even simpler?!?

Yes: $\langle T, S \rangle = \mathrm{SL}(2, \mathbb{Z})$. So, finally,

$$\theta \mid \alpha = \theta, \qquad \alpha \in \mathrm{SL}(2, \mathbb{Z}).$$

An analytic function on $\mathbb{H}^2$ satisfying this equation, and having a Fourier expansion like that of $\theta$, is a **modular form** (of weight $m/2$ for $\mathrm{SL}(2, \mathbb{Z})$).

# The meaning of the functional equations, continued

We can now rewrite the functional equations very simply as

$$\theta \mid T = \theta, \qquad \theta \mid S = \theta.$$

Moreover, since "slash" $\mid$ is a right action we can even say that

$$\theta \mid \alpha = \theta$$

for $\alpha$ in the subgroup $\langle T, S \rangle$ of $\mathrm{SL}(2, \mathbb{R})$ generated by $T$ and $S$.

But what is $\langle T, S \rangle$? Can this get even simpler?!?

Yes: $\langle T, S \rangle = \mathrm{SL}(2, \mathbb{Z})$. So, finally,

$$\theta \mid \alpha = \theta, \qquad \alpha \in \mathrm{SL}(2, \mathbb{Z}).$$

An analytic function on $\mathbb{H}^2$ satisfying this equation, and having a Fourier expansion like that of $\theta$, is a **modular form** (of weight $m/2$ for $\mathrm{SL}(2, \mathbb{Z})$).

# The meaning of the functional equations, continued

We can now rewrite the functional equations very simply as

$$\theta \mid T = \theta, \qquad \theta \mid S = \theta.$$

Moreover, since "slash" $\mid$ is a right action we can even say that

$$\theta \mid \alpha = \theta$$

for $\alpha$ in the subgroup $\langle T, S \rangle$ of $\mathrm{SL}(2, \mathbb{R})$ generated by $T$ and $S$.

But what is $\langle T, S \rangle$? Can this get even simpler?!?

Yes: $\langle T, S \rangle = \mathrm{SL}(2, \mathbb{Z})$. So, finally,

$$\theta \mid \alpha = \theta, \qquad \alpha \in \mathrm{SL}(2, \mathbb{Z}).$$

An analytic function on $\mathbb{H}^2$ satisfying this equation, and having a Fourier expansion like that of $\theta$, is a **modular form** (of weight $m/2$ for $\mathrm{SL}(2, \mathbb{Z})$).

# The meaning of the functional equations, continued

We can now rewrite the functional equations very simply as

$$\theta \mid T = \theta, \qquad \theta \mid S = \theta.$$

Moreover, since "slash" $\mid$ is a right action we can even say that

$$\theta \mid \alpha = \theta$$

for $\alpha$ in the subgroup $\langle T, S \rangle$ of $\mathrm{SL}(2, \mathbb{R})$ generated by $T$ and $S$.

But what is $\langle T, S \rangle$? Can this get even simpler?!?

Yes: $\langle T, S \rangle = \mathrm{SL}(2, \mathbb{Z})$. So, finally,

$$\theta \mid \alpha = \theta, \qquad \alpha \in \mathrm{SL}(2, \mathbb{Z}).$$

An analytic function on $\mathbb{H}^2$ satisfying this equation, and having a Fourier expansion like that of $\theta$, is a **modular form** (of weight $m/2$ for $\mathrm{SL}(2, \mathbb{Z})$).

# Back to our problem

We found that $\theta$ satisfies an amazing functional equation.

But can this actual help us determine the sequence $a(n)$?

The answer turns out to be yes (for $m = 8$ and $m = 16$), for two reasons.

Let

$$M_{m/2} = \text{the } \mathbb{C} \text{ vector space of modular forms of weight } m/2 \text{ for } \mathrm{SL}(2, \mathbb{Z}).$$

Then:

- $\dim M_{m/2} < \infty$, and $\dim M_{m/2}$ is known.
- There are other ways to get elements of $M_{m/2}$.

Let's first consider $\dim M_{m/2}$.

# Back to our problem

We found that $\theta$ satisfies an amazing functional equation.

But can this actual help us determine the sequence $a(n)$?

The answer turns out to be yes (for $m = 8$ and $m = 16$), for two reasons.

Let

$$M_{m/2} = \text{the } \mathbb{C} \text{ vector space of modular forms of weight } m/2 \text{ for } \mathrm{SL}(2, \mathbb{Z}).$$

Then:

- $\dim M_{m/2} < \infty$, and $\dim M_{m/2}$ is known.
- There are other ways to get elements of $M_{m/2}$.

Let's first consider $\dim M_{m/2}$.

# Back to our problem

We found that $\theta$ satisfies an amazing functional equation.

But can this actual help us determine the sequence $a(n)$?

The answer turns out to be yes (for $m = 8$ and $m = 16$), for two reasons.

Let

$$M_{m/2} = \text{the } \mathbb{C} \text{ vector space of modular forms of weight } m/2 \text{ for } \mathrm{SL}(2, \mathbb{Z}).$$

Then:

- $\dim M_{m/2} < \infty$, and $\dim M_{m/2}$ is known.
- There are other ways to get elements of $M_{m/2}$.

Let's first consider $\dim M_{m/2}$.

# Back to our problem

We found that $\theta$ satisfies an amazing functional equation.

But can this actual help us determine the sequence $a(n)$?

The answer turns out to be yes (for $m = 8$ and $m = 16$), for two reasons.

Let

$$M_{m/2} = \begin{array}{c}\text{the } \mathbb{C} \text{ vector space of modular forms} \\ \text{of weight } m/2 \text{ for } \mathrm{SL}(2, \mathbb{Z}).\end{array}$$

Then:

- $\dim M_{m/2} < \infty$, and $\dim M_{m/2}$ is known.
- There are other ways to get elements of $M_{m/2}$.

Let's first consider $\dim M_{m/2}$.

# Back to our problem

We found that $\theta$ satisfies an amazing functional equation.

But can this actual help us determine the sequence $a(n)$?

The answer turns out to be yes (for $m = 8$ and $m = 16$), for two reasons.

Let

$$M_{m/2} = \begin{array}{c}\text{the } \mathbb{C} \text{ vector space of modular forms} \\ \text{of weight } m/2 \text{ for } \mathrm{SL}(2, \mathbb{Z}).\end{array}$$

Then:

- $\dim M_{m/2} < \infty$, and $\dim M_{m/2}$ is known.
- There are other ways to get elements of $M_{m/2}$.

Let's first consider $\dim M_{m/2}$.

# Back to our problem

We found that $\theta$ satisfies an amazing functional equation.

But can this actual help us determine the sequence $a(n)$?

The answer turns out to be yes (for $m = 8$ and $m = 16$), for two reasons.

Let

$$M_{m/2} = \begin{array}{c}\text{the } \mathbb{C} \text{ vector space of modular forms} \\ \text{of weight } m/2 \text{ for } \mathrm{SL}(2, \mathbb{Z}).\end{array}$$

Then:

- $\dim M_{m/2} < \infty$, and $\dim M_{m/2}$ is known.
- There are other ways to get elements of $M_{m/2}$.

Let's first consider $\dim M_{m/2}$.

# Back to our problem

We found that $\theta$ satisfies an amazing functional equation.

But can this actual help us determine the sequence $a(n)$?

The answer turns out to be yes (for $m = 8$ and $m = 16$), for two reasons.

Let

$$M_{m/2} = \begin{array}{c}\text{the } \mathbb{C} \text{ vector space of modular forms} \\ \text{of weight } m/2 \text{ for } \mathrm{SL}(2, \mathbb{Z}).\end{array}$$

Then:

- $\dim M_{m/2} < \infty$, and $\dim M_{m/2}$ is known.
- There are other ways to get elements of $M_{m/2}$.

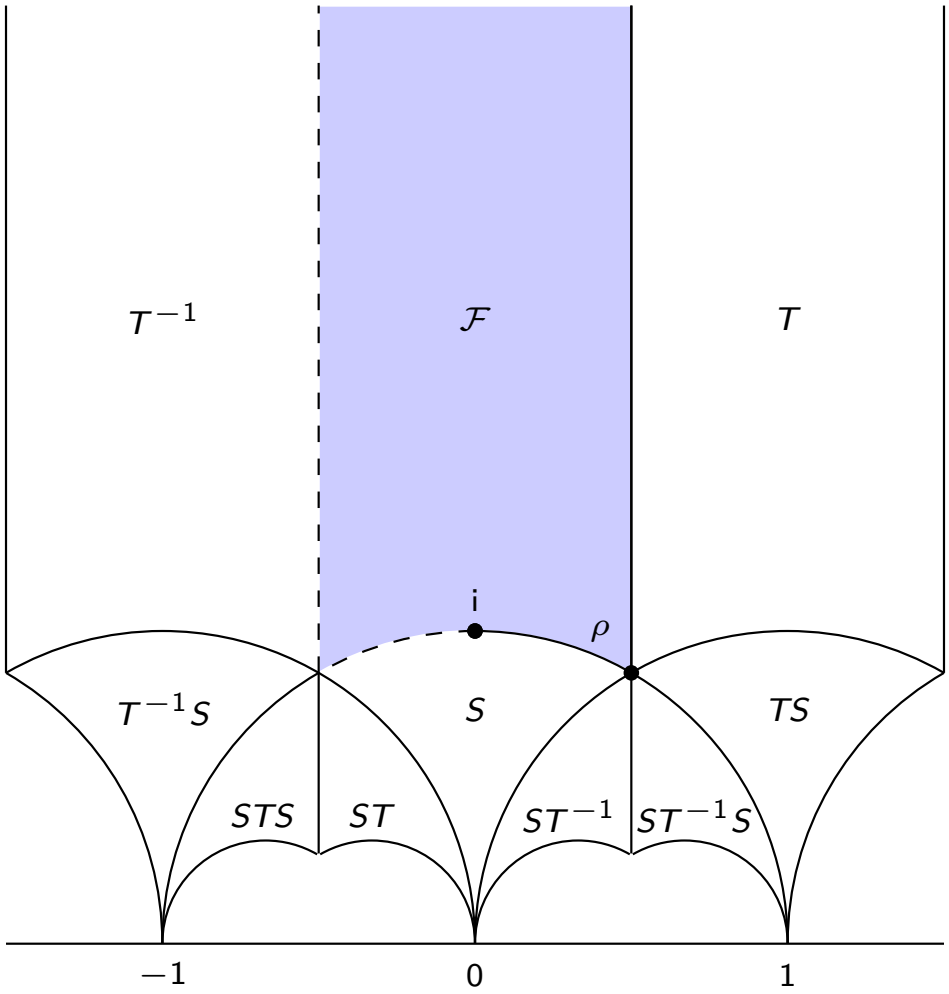
Let's first consider $\dim M_{m/2}$.

# The residue formula

To understand $\dim M_{m/2}$ it's helpful to first understand the action of $\mathrm{SL}(2,\mathbb{Z})$ on $\mathbb{H}^2$.
Let $\mathcal{F}$ be as drawn. Then $\mathcal{F}$ is a **fundamental domain**:

- every point of $\mathbb{H}^2$ is equivalent via $\mathrm{SL}(2,\mathbb{Z})$ to a point of $\mathcal{F}$;
- distinct points of $\mathcal{F}$ are inequivalent.

In fact, we obtain a tesselation of $\mathbb{H}^2$ in terms of hyperbolic triangles that are the images of $\mathcal{F}$ under $\mathrm{SL}(2,\mathbb{Z})$, as illustrated.



# The residue formula, continued

Now let $f \in M_{m/2}$ with $f \neq 0$, and let

$$f(z) = \sum_{n=0}^{\infty} b(n) q^n$$

be the Fourier expansion of $f$. Define

$$v_\infty(f) = \text{smallest } n \text{ such that } b(n) \neq 0.$$

For example, $v_\infty(\theta) = 0$.

Also, for $p \in \mathbb{H}^2$, let $v_p(f)$ be the order of vanishing of $f$ at $p$.

Using the residue theorem one can then prove the **residue formula**:

$$v_\infty(f) + \frac{1}{2} v_i(f) + \frac{1}{3} v_\rho(f) + \sum_{\substack{p \in \mathcal{F} \\ p \neq i, \rho}} v_p(f) = \frac{m}{24}.$$

# The residue formula, continued

Now let $f \in M_{m/2}$ with $f \neq 0$, and let

$$f(z) = \sum_{n=0}^{\infty} b(n) q^n$$

be the Fourier expansion of $f$. Define

$$v_\infty(f) = \text{smallest } n \text{ such that } b(n) \neq 0.$$

For example, $v_\infty(\theta) = 0$.

Also, for $p \in \mathbb{H}^2$, let $v_p(f)$ be the order of vanishing of $f$ at $p$.

Using the residue theorem one can then prove the **residue formula**:

$$v_\infty(f) + \frac{1}{2} v_i(f) + \frac{1}{3} v_\rho(f) + \sum_{\substack{p \in \mathcal{F} \\ p \neq i, \rho}} v_p(f) = \frac{m}{24}.$$

# The residue formula, continued

Now let $f \in M_{m/2}$ with $f \neq 0$, and let

$$f(z) = \sum_{n=0}^{\infty} b(n) q^n$$

be the Fourier expansion of $f$. Define

$$v_\infty(f) = \text{smallest } n \text{ such that } b(n) \neq 0.$$

For example, $v_\infty(\theta) = 0$.

Also, for $p \in \mathbb{H}^2$, let $v_p(f)$ be the order of vanishing of $f$ at $p$.

Using the residue theorem one can then prove the **residue formula**:

$$v_\infty(f) + \frac{1}{2} v_i(f) + \frac{1}{3} v_\rho(f) + \sum_{\substack{p \in \mathcal{F} \\ p \neq i, \rho}} v_p(f) = \frac{m}{24}.$$

# The residue formula, continued

Now let $f \in M_{m/2}$ with $f \neq 0$, and let

$$f(z) = \sum_{n=0}^{\infty} b(n) q^n$$

be the Fourier expansion of $f$. Define

$$v_\infty(f) = \text{smallest } n \text{ such that } b(n) \neq 0.$$

For example, $v_\infty(\theta) = 0$.

Also, for $p \in \mathbb{H}^2$, let $v_p(f)$ be the order of vanishing of $f$ at $p$.

Using the residue theorem one can then prove the **residue formula**:

$$v_\infty(f) + \frac{1}{2} v_i(f) + \frac{1}{3} v_\rho(f) + \sum_{\substack{p \in \mathcal{F} \\ p \neq i, \rho}} v_p(f) = \frac{m}{24}.$$

# $\dim M_{m/2} = 1$ for $m = 8$ and $m = 16$

We claim that this yields $\dim M_{m/2} = 1$ for $m = 8$ and $m = 16$.

Since $\theta \in M_{m/2}$ we already know $\dim M_{m/2} \geq 1$.

Suppose that $\dim M_{m/2} > 1$.

We can then make a non-zero element $f$ of $M_{m/2}$ with $v_\infty(f) \geq 1$.

But then

$$1 \leq v_\infty(f) + \frac{1}{2} v_i(f) + \frac{1}{3} v_\rho(f) + \sum_{\substack{p \in \mathcal{F} \\ p \neq i, \rho}} v_p(f) = \frac{m}{24} < 1,$$

a contradiction!

Hence,

$$\dim M_{m/2} = 1 \text{ for } m = 8 \text{ and } m = 16.$$

# $\dim M_{m/2} = 1$ for $m = 8$ and $m = 16$

We claim that this yields $\dim M_{m/2} = 1$ for $m = 8$ and $m = 16$.

Since $\theta \in M_{m/2}$ we already know $\dim M_{m/2} \geq 1$.

Suppose that $\dim M_{m/2} > 1$.

We can then make a non-zero element $f$ of $M_{m/2}$ with $v_\infty(f) \geq 1$.

But then

$$1 \leq v_\infty(f) + \frac{1}{2} v_i(f) + \frac{1}{3} v_\rho(f) + \sum_{\substack{p \in \mathcal{F} \\ p \neq i, \rho}} v_p(f) = \frac{m}{24} < 1,$$

a contradiction!

Hence,

$$\dim M_{m/2} = 1 \text{ for } m = 8 \text{ and } m = 16.$$

# $\dim M_{m/2} = 1$ for $m = 8$ and $m = 16$

We claim that this yields $\dim M_{m/2} = 1$ for $m = 8$ and $m = 16$.

Since $\theta \in M_{m/2}$ we already know $\dim M_{m/2} \geq 1$.

Suppose that $\dim M_{m/2} > 1$.

We can then make a non-zero element $f$ of $M_{m/2}$ with $v_\infty(f) \geq 1$.

But then

$$1 \leq v_\infty(f) + \frac{1}{2} v_i(f) + \frac{1}{3} v_\rho(f) + \sum_{\substack{p \in \mathcal{F} \\ p \neq i, \rho}} v_p(f) = \frac{m}{24} < 1,$$

a contradiction!

Hence,

$$\dim M_{m/2} = 1 \text{ for } m = 8 \text{ and } m = 16.$$

# $\dim M_{m/2} = 1$ for $m = 8$ and $m = 16$

We claim that this yields $\dim M_{m/2} = 1$ for $m = 8$ and $m = 16$.

Since $\theta \in M_{m/2}$ we already know $\dim M_{m/2} \geq 1$.

Suppose that $\dim M_{m/2} > 1$.

We can then make a non-zero element $f$ of $M_{m/2}$ with $v_\infty(f) \geq 1$.

But then

$$1 \leq v_\infty(f) + \frac{1}{2} v_i(f) + \frac{1}{3} v_\rho(f) + \sum_{\substack{p \in \mathcal{F} \\ p \neq i, \rho}} v_p(f) = \frac{m}{24} < 1,$$

a contradiction!

Hence,

$$\dim M_{m/2} = 1 \text{ for } m = 8 \text{ and } m = 16.$$

# $\dim M_{m/2} = 1$ for $m = 8$ and $m = 16$

We claim that this yields $\dim M_{m/2} = 1$ for $m = 8$ and $m = 16$.

Since $\theta \in M_{m/2}$ we already know $\dim M_{m/2} \geq 1$.

Suppose that $\dim M_{m/2} > 1$.

We can then make a non-zero element $f$ of $M_{m/2}$ with $v_\infty(f) \geq 1$.

But then

$$1 \leq v_\infty(f) + \frac{1}{2} v_i(f) + \frac{1}{3} v_\rho(f) + \sum_{\substack{p \in \mathcal{F} \\ p \neq i, \rho}} v_p(f) = \frac{m}{24} < 1,$$

a contradiction!

Hence,

$$\dim M_{m/2} = 1 \text{ for } m = 8 \text{ and } m = 16.$$

# $\dim M_{m/2} = 1$ for $m = 8$ and $m = 16$

We claim that this yields $\dim M_{m/2} = 1$ for $m = 8$ and $m = 16$.

Since $\theta \in M_{m/2}$ we already know $\dim M_{m/2} \geq 1$.

Suppose that $\dim M_{m/2} > 1$.

We can then make a non-zero element $f$ of $M_{m/2}$ with $v_\infty(f) \geq 1$.

But then

$$1 \leq v_\infty(f) + \frac{1}{2}v_i(f) + \frac{1}{3}v_\rho(f) + \sum_{\substack{p \in \mathcal{F} \\ p \neq i, \rho}} v_p(f) = \frac{m}{24} < 1,$$

a contradiction!

Hence,

$$\dim M_{m/2} = 1 \text{ for } m = 8 \text{ and } m = 16.$$

# Another construction

So now we know that dim $M_{m/2} = 1$ if $m = 8$ or $m = 16$.

Is there another way to construct elements of $M_{m/2}$?

Yes. Define

$$E(z) = \frac{1}{2\zeta(m/2)} \sum_{\substack{(a,b)\in\mathbb{Z}^2, \\ (a,b)\neq(0,0)}} \frac{1}{(az+b)^{m/2}}$$

for $z \in \mathbb{H}^2$. This is an **Eisenstein series**.

This converges and satisfies the two functional equations.

Moreover, it has a Fourier expansion so it's in $M_{m/2}$.

From complex analysis one has

$$\frac{1}{z} + \sum_{b=1}^{\infty} \left( \frac{1}{z+b} + \frac{1}{z-b} \right) = \pi i - 2\pi i \sum_{n=0}^{\infty} q^n.$$

# Another construction

So now we know that dim $M_{m/2} = 1$ if $m = 8$ or $m = 16$.

Is there another way to construct elements of $M_{m/2}$?

Yes. Define

$$E(z) = \frac{1}{2\zeta(m/2)} \sum_{\substack{(a,b)\in\mathbb{Z}^2,\\ (a,b)\neq(0,0)}} \frac{1}{(az+b)^{m/2}}$$

for $z \in \mathbb{H}^2$. This is an **Eisenstein series**.

This converges and satisfies the two functional equations.

Moreover, it has a Fourier expansion so it's in $M_{m/2}$.

From complex analysis one has

$$\frac{1}{z} + \sum_{b=1}^{\infty} \left( \frac{1}{z+b} + \frac{1}{z-b} \right) = \pi i - 2\pi i \sum_{n=0}^{\infty} q^n.$$

# Another construction

So now we know that $\dim M_{m/2} = 1$ if $m = 8$ or $m = 16$.

Is there another way to construct elements of $M_{m/2}$?

Yes. Define

$$E(z) = \frac{1}{2\zeta(m/2)} \sum_{\substack{(a,b)\in\mathbb{Z}^2,\\ (a,b)\neq(0,0)}} \frac{1}{(az+b)^{m/2}}$$

for $z \in \mathbb{H}^2$. This is an **Eisenstein series**.

This converges and satisfies the two functional equations.

Moreover, it has a Fourier expansion so it's in $M_{m/2}$.

From complex analysis one has

$$\frac{1}{z} + \sum_{b=1}^{\infty} \left( \frac{1}{z+b} + \frac{1}{z-b} \right) = \pi i - 2\pi i \sum_{n=0}^{\infty} q^n.$$

# Another construction

So now we know that dim $M_{m/2} = 1$ if $m = 8$ or $m = 16$.

Is there another way to construct elements of $M_{m/2}$?

Yes. Define

$$E(z) = \frac{1}{2\zeta(m/2)} \sum_{\substack{(a,b)\in\mathbb{Z}^2, \\ (a,b)\neq(0,0)}} \frac{1}{(az+b)^{m/2}}$$

for $z \in \mathbb{H}^2$. This is an **Eisenstein series**.

This converges and satisfies the two functional equations.

Moreover, it has a Fourier expansion so it's in $M_{m/2}$.

From complex analysis one has

$$\frac{1}{z} + \sum_{b=1}^{\infty} \left( \frac{1}{z+b} + \frac{1}{z-b} \right) = \pi i - 2\pi i \sum_{n=0}^{\infty} q^n.$$

# Another construction

So now we know that dim $M_{m/2} = 1$ if $m = 8$ or $m = 16$.

Is there another way to construct elements of $M_{m/2}$?

Yes. Define

$$E(z) = \frac{1}{2\zeta(m/2)} \sum_{\substack{(a,b)\in\mathbb{Z}^2,\\ (a,b)\neq(0,0)}} \frac{1}{(az+b)^{m/2}}$$

for $z \in \mathbb{H}^2$. This is an **Eisenstein series**.

This converges and satisfies the two functional equations.

Moreover, it has a Fourier expansion so it's in $M_{m/2}$.

From complex analysis one has

$$\frac{1}{z} + \sum_{b=1}^{\infty} \left( \frac{1}{z+b} + \frac{1}{z-b} \right) = \pi i - 2\pi i \sum_{n=0}^{\infty} q^n.$$

# Another construction

So now we know that dim $M_{m/2} = 1$ if $m = 8$ or $m = 16$.

Is there another way to construct elements of $M_{m/2}$?

Yes. Define

$$E(z) = \frac{1}{2\zeta(m/2)} \sum_{\substack{(a,b)\in\mathbb{Z}^2, \\ (a,b)\neq(0,0)}} \frac{1}{(az+b)^{m/2}}$$

for $z \in \mathbb{H}^2$. This is an **Eisenstein series**.

This converges and satisfies the two functional equations.

Moreover, it has a Fourier expansion so it's in $M_{m/2}$.

From complex analysis one has

$$\frac{1}{z} + \sum_{b=1}^{\infty} \left( \frac{1}{z+b} + \frac{1}{z-b} \right) = \pi i - 2\pi i \sum_{n=0}^{\infty} q^n.$$

# Another construction, continued

Some calculations now show that

$$E(z) = 1 + \frac{(2\pi i)^{m/2}}{2\zeta(m/2)(m/2-1)!} \sum_{n=1}^{\infty} \sigma_{m/2-1}(n) q^n,$$

where

$$\sigma_{m/2-1}(n) = \begin{array}{l} \text{sum of the positive divisors of } n, \\ \text{each raised to the } m/2-1 \text{ power.} \end{array}$$

When $m = 8$ we get

$$E(z) = 1 + 240 \sum_{n=1}^{\infty} \sigma_3(n) q^n,$$

and when $m = 16$ we get

$$E(z) = 1 + 480 \sum_{n=1}^{\infty} \sigma_7(n) q^n.$$

# The solution

We are now ready to solve the problem of determining the $a(n)$ when $m = 8$ or $m = 16$.

Since $\dim M_{m/2} = 1$ when $m = 8$ or $m = 16$, we must have

$$\theta(z) = cE(z)$$

for some $c \in \mathbb{C}$. But we know that $a(0) = 1$; comparing Fourier expansions, we get $c = 1$.

Thus the solution is $a(0) = 1$, and if $n > 0$, then

$$a(n) = \begin{array}{c} \#\text{ integral} \\ \text{solutions} \\ \text{to} \\ \text{Q(x)=2n} \end{array} = \begin{cases} 240 \times \left( \begin{array}{l} \text{sum of the cubes of the} \\ \text{positive divisors of } n \text{ if } m = 8 \end{array} \right), \\ 480 \times \left( \begin{array}{l} \text{sum of the seventh powers of the} \\ \text{positive divisors of } n \text{ if } m = 16 \end{array} \right). \end{cases}$$

# The solution

We are now ready to solve the problem of determining the $a(n)$ when $m = 8$ or $m = 16$.

Since $\dim M_{m/2} = 1$ when $m = 8$ or $m = 16$, we must have

$$\theta(z) = cE(z)$$

for some $c \in \mathbb{C}$. But we know that $a(0) = 1$; comparing Fourier expansions, we get $c = 1$.

Thus the solution is $a(0) = 1$, and if $n > 0$, then

$$a(n) = \begin{array}{c} \#\text{ integral} \\ \text{solutions} \\ \text{to} \\ \text{Q(x)=2n} \end{array} = \begin{cases} 240 \times \left( \begin{array}{l} \text{sum of the cubes of the} \\ \text{positive divisors of } n \text{ if } m = 8 \end{array} \right), \\ 480 \times \left( \begin{array}{l} \text{sum of the seventh powers of the} \\ \text{positive divisors of } n \text{ if } m = 16 \end{array} \right). \end{cases}$$

# The solution

We are now ready to solve the problem of determining the $a(n)$ when $m = 8$ or $m = 16$.

Since $\dim M_{m/2} = 1$ when $m = 8$ or $m = 16$, we must have

$$\theta(z) = cE(z)$$

for some $c \in \mathbb{C}$. But we know that $a(0) = 1$; comparing Fourier expansions, we get $c = 1$.

Thus the solution is $a(0) = 1$, and if $n > 0$, then

$$a(n) = \begin{array}{c} \#\text{ integral} \\ \text{solutions} \\ \text{to} \\ \text{Q(x)=2n} \end{array} = \begin{cases} 240 \times \left( \begin{array}{l} \text{sum of the cubes of the} \\ \text{positive divisors of } n \text{ if } m = 8 \end{array} \right), \\ 480 \times \left( \begin{array}{l} \text{sum of the seventh powers of the} \\ \text{positive divisors of } n \text{ if } m = 16 \end{array} \right). \end{cases}$$

# The solution, continued

The theta series are now

$$\begin{aligned} m = 8: &\qquad \theta(z) = 1 + 240\, q + 2160\, q^2 + 6720\, q^3 + \cdots \\ m = 16: &\qquad \theta(z) = 1 + 480\, q + 61920\, q^2 + 1050240\, q^3 + \cdots . \end{aligned}$$

Interestingly, if $m = 16$, then the number of integral solutions to $Q(x) = 2n$ is the same for the two non-equivalent $Q(x)$.

# The big picture

This was a nice solution!

But how relevant are modular forms, really?

In fact, modular forms are connected to almost all parts of mathematics.

One way to see a hint of this is to notice that $\mathrm{SL}(2,\mathbb{R})$ acts transitively on $\mathbb{H}^2$, and that the stabilizer of $i$ is

$$\mathrm{SO}(2,\mathbb{R}) = \left\{ \begin{bmatrix} a & b \\ -a & b \end{bmatrix} : a^2 + b^2 = 1 \right\}.$$

Thus,

$$\mathrm{SL}(2,\mathbb{R})/\mathrm{SO}(2,\mathbb{R}) \xrightarrow{\sim} \mathbb{H}^2, \qquad g\mathrm{SO}(2,\mathbb{R}) \mapsto g \cdot i.$$

Given a modular form $f$ of weight $k$, one can then define a corresponding function

$$\phi : \mathrm{SL}(2,\mathbb{R}) \to \mathbb{C}, \qquad \phi(g) = f(g \cdot i) j(g,i)^{-k}, \qquad g \in \mathrm{SL}(2,\mathbb{R}).$$

# The big picture

This was a nice solution!

But how relevant are modular forms, really?

In fact, modular forms are connected to almost all parts of mathematics.

One way to see a hint of this is to notice that $\mathrm{SL}(2,\mathbb{R})$ acts transitively on $\mathbb{H}^2$, and that the stabilizer of $i$ is

$$\mathrm{SO}(2,\mathbb{R}) = \left\{ \begin{bmatrix} a & b \\ -a & b \end{bmatrix} : a^2 + b^2 = 1 \right\}.$$

Thus,

$$\mathrm{SL}(2,\mathbb{R})/\mathrm{SO}(2,\mathbb{R}) \xrightarrow{\sim} \mathbb{H}^2, \qquad g\mathrm{SO}(2,\mathbb{R}) \mapsto g \cdot i.$$

Given a modular form $f$ of weight $k$, one can then define a corresponding function

$$\phi : \mathrm{SL}(2,\mathbb{R}) \to \mathbb{C}, \qquad \phi(g) = f(g \cdot i) j(g,i)^{-k}, \qquad g \in \mathrm{SL}(2,\mathbb{R}).$$

# The big picture

This was a nice solution!

But how relevant are modular forms, really?

In fact, modular forms are connected to almost all parts of mathematics.

One way to see a hint of this is to notice that $\mathrm{SL}(2,\mathbb{R})$ acts transitively on $\mathbb{H}^2$, and that the stabilizer of $i$ is

$$\mathrm{SO}(2,\mathbb{R}) = \left\{ \begin{bmatrix} a & b \\ -a & b \end{bmatrix} : a^2 + b^2 = 1 \right\}.$$

Thus,

$$\mathrm{SL}(2,\mathbb{R})/\mathrm{SO}(2,\mathbb{R}) \xrightarrow{\sim} \mathbb{H}^2, \qquad g\mathrm{SO}(2,\mathbb{R}) \mapsto g \cdot i.$$

Given a modular form $f$ of weight $k$, one can then define a corresponding function

$$\phi : \mathrm{SL}(2,\mathbb{R}) \to \mathbb{C}, \qquad \phi(g) = f(g \cdot i) j(g,i)^{-k}, \qquad g \in \mathrm{SL}(2,\mathbb{R}).$$

# The big picture, continued

The function $\phi : \mathrm{SL}(2,\mathbb{R}) \to \mathbb{C}$ has a number of properties, including that

$$\phi(\alpha g) = \phi(g), \qquad \alpha \in \mathrm{SL}(2,\mathbb{Z}), \quad g \in \mathrm{SL}(2,\mathbb{R}).$$

In fact

$$\phi \in L^2(\mathrm{SL}(2,\mathbb{Z})\backslash \mathrm{SL}(2,\mathbb{R})).$$

Since $L^2(\mathrm{SL}(2,\mathbb{Z})\backslash \mathrm{SL}(2,\mathbb{R}))$ is a unitary representation of $\mathrm{SL}(2,\mathbb{R})$ via right translation, we find that the study of modular forms is closely related to the study of certain (automorphic) representations of $\mathrm{SL}(2,\mathbb{R})$.

In practice, $\mathbb{R}$ is replaced by $\mathbb{A}$, the adeles of $\mathbb{Q}$, so that all completions of $\mathbb{Q}$ are on the same footing, and $\mathrm{SL}(2)$ is replaced by a reductive linear algebraic group $G$ defined over $\mathbb{Q}$. In this setting there is big network of ideas connecting automorphic representations, Shimura varieties, and Galois representations.

At the same time, plenty of work is still being done in the classical setting.

# Further reading and viewing

Quanta magazine

www.quantamagazine.org

is an excellent source for expository articles about mathematics, physics, and other disciplines. This magazine is supported by the Simons Foundation.

Quanta often has interesting stories about modular forms, including an article about the connections between the representation theory of sporadic finite simple groups, string theory, and modular forms.

Search for "modular forms" at the Quanta website.

Quanta also has a nice YouTube channel.

At the channel search for "The Biggest Project in Modern Mathematics". This video is about modular forms and their applications.