Generating Functions, Partitions, and $q$-series: An Introduction to Classical Modular Forms

Edray Herber Goins

MA 59800-614-27988: Classical Modular Forms
Department of Mathematics
Purdue University

June 28, 2016
Abstract

It is natural to count the number of objects placed into a geometric shape. For example, “triangular numbers” are the number objects that can form an equilateral triangle, while “pentagonal numbers” are the number of objects that can form a regular pentagon. Similarly, it is natural to ask how to partition a natural number into smaller parts. In the 1700’s, the German mathematician Leonhard Euler found a remarkable relationship between these two sets of numbers. Euler’s Pentagonal Number Theorem paved the way for the concept of a $q$-series as a generating function for other interesting sequences of numbers.

In 1919, the English mathematician Godfrey Harold Hardy went to visit his ill friend Srinivasa Ramanujan in the hospital. Hardy told Ramanujan that had ridden in taxi-cab No. 1729, and remarked that the number seemed to be rather a dull one. Ramanujan countered the number is very interesting as it is the smallest number expressible as the sum of two positive cubes in two different ways. Hardy was working with Ramanujan to understand some of his pulchritudinous identities involving the coefficients of a certain “modular discriminant.” This specific $q$-series has a transformation property which led to the theory of modular forms.

In this introductory talk, we’ll present various applications of classical modular forms to questions which naturally arise in combinatorics, algebra, and number theory. In particular, we’ll discuss properties of quadratic forms (why is every positive integer the sum of four squares?), cubic forms (what are “taxi-cab” numbers?) and congruences among the coefficients (why is Ramanujan’s tau function so closely related to the divisor function?).
Outline

1. Generating Functions, Partitions, and $q$-Series
   - Figurate Numbers
   - Partition Function
   - $q$-Series

2. Modular Forms
   - Riemann Zeta Function
   - Special Values of the Riemann Zeta Function
   - Modular Forms, Eisenstein Series, and Cusp Forms

3. Applications
   - Representing Integers as the Sums of Squares
   - Ramanujan Tau Function
   - Elliptic Curves and the Taniyama-Shimura-Weil Conjecture
A **triangular number** counts the number of objects that can form an equilateral triangle. The $n$th triangular number $T_n$ is the number of dots composing a triangle with $n$ dots on a side.

$$T_1 = 1 \quad T_2 = 3 \quad T_3 = 6 \quad T_4 = 10$$

$$T_5 = 15 \quad T_6 = 21$$

Applications

Handshake Problem

\( T_n \) is the total number of handshakes required if each person in a room with \( n + 1 \) people shakes hands once with each person.

Proposition

\( T_n \) is the number of edges in a complete graph \( K_n \) of order \( n \).

There are other applications at Sloan’s Online Encyclopedia of Integer Sequences: http://oeis.org/A000217
Proposition

Let \( T_n \) denote the \( n \)th triangular number.

- \( T_n = n + (n - 1) + \cdots + 2 + 1 = n(n + 1)/2. \)
- The consecutive sum \( T_n + T_{n-1} = n^2 \) is always a perfect square.
- The consecutive difference of squares \( T_n^2 - T_{n-1}^2 = n^3 \) is a perfect cube.
- \( \sum_{n=0}^{\infty} T_n q^n = \frac{q}{(1 - q)^3} \) is a generating function for \( T_n \).

To see the last assertion, differentiate the Geometric Series twice:

\[
\sum_{n=0}^{\infty} q^{n+1} = \frac{q}{1 - q}
\]

\[
\sum_{n=0}^{\infty} (n + 1) q^n = \frac{1}{(1 - q)^2}
\]

\[
\sum_{n=0}^{\infty} n(n + 1) q^{n-1} = \frac{2}{(1 - q)^3} \quad \Rightarrow \quad \sum_{n=0}^{\infty} \frac{n(n + 1)}{2} q^n = \frac{q}{(1 - q)^3}
\]
Figurate Numbers

Definition

A **figurate number** is a natural number that can be represented by a regular geometrical arrangement of equally spaced points. If the arrangement forms a regular polygon, the number is called a polygonal number.

Some examples of polygonal numbers are:

- **triangular numbers** \( T_n \),
- **square numbers** \( S_n \),
- **pentagonal numbers** \( G_n \), and
- **hexagonal numbers** \( H_n \).

http://mathworld.wolfram.com/FigurateNumber.html
Square Numbers

Proposition

Let $S_n$ denote the $n$th square number.

- $S_n = n^2$.
- $\sum_{n=1}^{\infty} S_n q^n = \frac{q(q+1)}{(1-q)^3}$ is a generating function for $S_n$.

To see why, consider the recursive relation:

- $S_1 = 1$
- $S_{n+1} = (2n + 1) + S_n$

$\implies S_n = \sum_{k=0}^{n-1} (2k + 1) = n^2$.

http://mathworld.wolfram.com/SquareNumber.html
Proposition

Let $G_n$ denote the $n$th pentagonal number.

- $G_n = \frac{n(3n - 1)}{2}$.

- $\sum_{n=1}^{\infty} G_n \ q^n = \frac{q(2q + 1)}{(1 - q)^3}$ is a generating function for $G_n$.

To see why, consider the recursive relation:

\[
G_1 = 1
\]
\[
G_{n+1} = (3n + 1) + G_n
\]

\[
\Rightarrow G_n = \sum_{k=0}^{n-1} (3k + 1) = \frac{n(3n - 1)}{2}.
\]

http://mathworld.wolfram.com/PentagonalNumber.html
Hexagonal Numbers

Proposition

Let $H_n$ denote the $n$th hexagonal number.

- $H_n = n(2n - 1)$.
- $\sum_{n=1}^{\infty} H_n q^n = \frac{q(3q + 1)}{(1 - q)^3}$ is a generating function for $H_n$.

To see why, consider the recursive relation:

$$H_1 = 1$$

$$H_{n+1} = (4n + 1) + H_n \implies H_n = \sum_{k=0}^{n-1} (4k + 1) = n(2n - 1).$$

http://mathworld.wolfram.com/HexagonalNumber.html
Do You See a Pattern?
Proposition

Let $N_n$ denote the $n$th figurate number associated to a regular $m$-gon.

\[ N_n = \frac{n((m-2)(n-1)+2)}{2}. \]

\[ \sum_{n=1}^{\infty} N_n q^n = \frac{q((m-3)q+1)}{(1-q)^3} \] is a generating function for $N_n$.

To see why, consider the recursive relation $N_{n+1} = ((m-2)n+1) + N_n$:

\[ N_n = \sum_{k=0}^{n-1} ((m-2)k + 1) = (m-2) \frac{n(n-1)}{2} + n. \]

To see the last assertion, differentiate the Geometric Series twice:

\[ \sum_{n=0}^{\infty} n q^n = \frac{q}{(1-q)^2} \]

\[ \sum_{n=0}^{\infty} \frac{n(n-1)}{2} q^n = \frac{q^2}{(1-q)^3} \quad \Rightarrow \quad \sum_{n=0}^{\infty} N_n q^n = \frac{(m-2)q^2}{(1-q)^3} + \frac{q}{(1-q)^2} \]
Leonhard Euler
April 15, 1707 – September 18, 1783
https://en.wikipedia.org/wiki/Leonhard_Euler
A partition of a natural number \( n \) is a way of writing \( n \) as a sum of positive integers. The number \( p_n \) is the number of partitions of \( n \).

Here are some examples:

- \( p_1 = 1 \) because there is only one partition of 1
- \( p_2 = 2 \) because there are two partitions of 2, namely \( 2 = 1 + 1 \)
- \( p_3 = 3 \) because there are three partitions of 3, namely \( 3 = 2 + 1 = 1 + 1 + 1 \)
- \( p_4 = 5 \) because there are five partitions of 4, namely \( 4 = 3 + 1 = 2 + 2 + 1 + 1 = 1 + 1 + 1 + 1 \)
- \( p_5 = 7 \) because there are seven partitions of 5, namely \( 5 = 4 + 1 = 3 + 2 = 3 + 1 + 1 = 2 + 2 + 1 = 2 + 1 + 1 + 1 = 1 + 1 + 1 + 1 + 1 \)

https://en.wikipedia.org/wiki/Partition_(number_theory)
Proposition (Leonhard Euler)

Let $p_n$ denote the number of partitions of $n$. It has the “generating function”

$$\sum_{n=0}^{\infty} p_n q^n = \prod_{m=1}^{\infty} \frac{1}{1 - q^m}.$$ 

To see why, first expand out the terms in the product as Geometric Series:

$$\prod_{m=1}^{\infty} \frac{1}{1 - q^m} = \prod_{m=1}^{\infty} \left( \sum_{e=0}^{\infty} q^{em} \right) = \sum_{n=0}^{\infty} N_n q^n$$

where $N_n$ is the number of ways we can express $n = \sum_{m=1}^{\infty} e_m m$ where each $m$ appears $e_m$ times. But these are just partitions of $n$, so $N_n = p_n$.

Remark: We do not know a nice closed-expression for $p_n$. 


Recall that two integers \( a \) and \( b \) are said to be “congruent modulo \( N \)” if \( b - a \) is a multiple of \( N \). We write \( a \equiv b \mod N \).

**Proposition (Srinivasa Ramanujan, 1910’s)**

- \( p_n \equiv 0 \mod 5 \) whenever \( n \equiv 4 \mod 5 \).
- \( p_n \equiv 0 \mod 7 \) whenever \( n \equiv 5 \mod 7 \).
- \( p_n \equiv 0 \mod 11 \) whenever \( n \equiv 6 \mod 11 \).

**Proposition (Arthur Oliver Lonsdale Atkin, 1960’s)**

\[ p_n \equiv 0 \mod 13 \] whenever \( n \equiv 237 \mod 11^3 \cdot 13 \).

**Proposition (Ken Ono, 2000; Scott Ahlgren and Ken Ono, 2001)**

- \( p_n \equiv 0 \mod 31 \) whenever \( n \equiv 30064597 \mod 4063467631 \).
- Let \( N \) be a positive integer relatively prime to 6. Then there exist integer \( n_0 \) and \( N_0 \) such that \( p_n \equiv 0 \mod N \) whenever \( n \equiv n_0 \mod N_0 \).

https://en.wikipedia.org/wiki/Ramanujan’s_congruences
Proposition (Leonhard Euler)

Denote \( G_n = \frac{n(3n-1)}{2} \) as the \( n \)th pentagonal number – for all integers \( n \). Then we have the identity

\[
\prod_{m=1}^{\infty} (1 - q^m) = \sum_{n \in \mathbb{Z}} (-1)^n q^{G_n}
\]

That is, we have the expansion

\[(1 - q)(1 - q^2)(1 - q^3) \cdots = 1 - q - q^2 + q^5 + q^7 - q^{12} - q^{15} + q^{22} + \cdots.\]

Corollary

\[
\left( \sum_{n=0}^{\infty} p_n q^n \right) \left( \sum_{n \in \mathbb{Z}} (-1)^n q^{G_n} \right) = 1.
\]

https://en.wikipedia.org/wiki/Pentagonal_number_theorem
Say that we have a sequence of numbers \( a_0, a_1, a_2, \ldots, a_n, \ldots \).

- The generating function
  \[
  f(q) = \sum_{n=0}^{\infty} a_n q^n
  \]
  is also called a \( q \)-series. It is a Maclaurin series in the variable \( q \).

- As a specific example, let \( N_n \) denote the \( n \)th figurate number associated to a regular \( m \)-gon. Then we have the closed-expressions
  \[
  N_n = \frac{n ((m - 2) (n - 1) + 2)}{2} \quad \text{and} \quad \sum_{n=1}^{\infty} N_n q^n = \frac{q ((m - 3) q + 1)}{(1 - q)^3}.
  \]

- Let \( p_n \) denote the number of partitions of \( n \) and \( G_n = n (3 n - 1)/2 \) as the \( n \)th Pentagonal number. Then we have the relation
  \[
  \left( \sum_{n=0}^{\infty} p_n q^n \right) \left( \sum_{n \in \mathbb{Z}} (-1)^n q^{G_n} \right) = 1.
  \]
Carl Gustav Jacob Jacobi
December 10, 1804 – February 18, 1851
https://en.wikipedia.org/wiki/Carl_Gustav_Jacob_Jacobi
The Pentagonal Number Theorem follows from the following general result:

**Proposition (Carl Gustav Jacob Jacobi, 1829)**

\[
\prod_{m=1}^{\infty} \left(1 - w^{2m}\right) \left(1 + z w^{2m-1}\right) \left(1 + z^{-1} w^{2m-1}\right) = \sum_{n \in \mathbb{Z}} z^n w^{n^2}.
\]

To see why, substitute \( z = -q^{-1/2} \) and \( w = q^{3/2} \):

\[
\prod_{m=1}^{\infty} \left(1 - w^{2m}\right) \left(1 + z w^{2m-1}\right) \left(1 + z^{-1} w^{2m-1}\right)
\]

\[
= \prod_{m=1}^{\infty} \left(1 - q^{3m}\right) \left(1 - q^{3m-2}\right) \left(1 - q^{3m-1}\right)
\]

\[
= \prod_{m=1}^{\infty} (1 - q^m)
\]

\[
\sum_{n \in \mathbb{Z}} z^n w^{n^2} = \sum_{n \in \mathbb{Z}} (-1)^n q^{G_n}
\]
Jacobi Triple Product

Proposition (Carl Gustav Jacob Jacobi, 1829)

\[
\prod_{m=1}^{\infty} \left(1 - w^{2m}\right) \left(1 + z w^{2m-1}\right) \left(1 + z^{-1} w^{2m-1}\right) = \sum_{n \in \mathbb{Z}} z^n w^{n^2}.
\]

We have a transformation property:

Corollary

For \( z = 1 \) and \( w = e^{-\pi t^2} \), denote the function

\[
\Theta(t) = \prod_{m=1}^{\infty} \left(1 - e^{-2m\pi t^2}\right) \left(1 + e^{(1-2m)\pi t^2}\right)^2 = 1 + 2 \sum_{n=1}^{\infty} e^{-\pi n^2 t^2}.
\]

- \( \Theta(1/t) = t \Theta(t) \) for all \( t > 0 \).
- \( \lim_{t \to \infty} \Theta(t) = 1 \).
Motivating Question

Consider the statement

\[ 1 + 2 + 3 + 4 + \cdots + n + \cdots = -\frac{1}{12}. \]

Is this absurd or does this actually make sense?

This is the subject of a YouTube video by Numberphile:

https://www.youtube.com/watch?feature=player_embedded&v=w-I6XTVZXww

as well as a New York Times article by Dennis Overbye featuring Ed Frenkel:

http://www.nytimes.com/2014/02/04/science/in-the-end-it-all-adds-up-to.html

“Theorem”

- \[ 1 + 2 + 3 + 4 + \cdots + n + \cdots = -\frac{1}{12}. \]
- \[ 1 + 2^3 + 3^3 + 4^3 + \cdots + n^3 + \cdots = +\frac{1}{120}. \]
- \[ 1 + 2^{2k-1} + 3^{2k-1} + 4^{2k-1} + \cdots + n^{2k-1} + \cdots = -\frac{B_{2k}}{2k}. \]
Consider the Riemann zeta function

\[ \zeta(s) = \sum_{n=1}^{\infty} \frac{1}{n^s} = \prod_{\text{primes } p} \frac{1}{1 - p^{-s}}. \]

**Theorem (Bernhard Riemann)**

For \( s \in \mathbb{C} \) satisfying \( \text{Re}(s) > 1 \), define the functions

\[ \Lambda(s) = \frac{1}{\pi^{s/2}} \Gamma \left( \frac{s}{2} \right) \zeta(s), \quad \Gamma(s) = \int_{0}^{\infty} e^{-t} t^{s-1} \, dt = (s-1)! \]

Consider those \( s \in \mathbb{C} \) which satisfy \( 0 < \text{Re}(s) < 1 \).

- \( \Lambda(1-s) = \Lambda(s) \).
- The Riemann zeta function satisfies the **functional equation**

\[ \zeta(1-s) = \frac{2}{(2\pi)^s} \cos \left( \frac{\pi s}{2} \right) \Gamma(s) \zeta(s). \]
Proof of Theorem

\[ \Theta(t) = \prod_{m=1}^{\infty} \left( 1 - e^{-2m\pi t^2} \right) \left( 1 + e^{(1-2m)\pi t^2} \right)^2 = 1 + 2 \sum_{n=1}^{\infty} e^{-\pi n^2 t^2}, \quad t > 0. \]

Lemma 1

\[ \int_0^{\infty} [\Theta(t) - 1] t^{s-1} dt = \Lambda(s) \text{ for } \text{Re}(s) > 1. \]

\[ \int_0^{\infty} [\Theta(t) - 1] t^{s-1} dt = \sum_{n=1}^{\infty} 2 \int_0^{\infty} e^{-\pi n^2 t^2} t^{s-1} dt = \frac{1}{\pi^{s/2}} \Gamma \left( \frac{s}{2} \right) \sum_{n=1}^{\infty} \frac{1}{n^s} = \Lambda(s). \]

Lemma 2

\[ \Lambda(s) = \Lambda(1 - s) \text{ when } 0 < \text{Re}(s) < 1. \]

Using Lemmas 1 and the identity \( \Theta(1/t) = t \Theta(t) \) we find that

\[ \Lambda(s) = \frac{1}{s(1-s)} + \int_1^{\infty} [\Theta(t) - 1] \left[ t^{-s} + t^{s-1} \right]. \]
Lemma 3 (Legendre’s Duplication Formula).

For \( s \in \mathbb{C} \) satisfying 0 < Re\((s)\) < 1,

\[
\Gamma(s) = \frac{2^{s-1}}{\sqrt{\pi}} \Gamma\left(\frac{s}{2}\right) \Gamma\left(\frac{1+s}{2}\right), \quad \Gamma\left(\frac{1-s}{2}\right) \Gamma\left(\frac{1+s}{2}\right) = \pi / \cos\left(\frac{\pi s}{2}\right)
\]

\[
\frac{\zeta(1-s)}{2 \cos\left(\frac{\pi s}{2}\right)} \Gamma(s) \zeta(s) = \frac{(2\pi)^s}{2 \cos\left(\frac{\pi s}{2}\right) \Gamma(s)} \cdot \frac{\pi^{(1-s)/2} \Lambda(1-s)}{\Gamma\left(\frac{1-s}{2}\right)} \cdot \frac{\pi^{s/2} \Lambda(s)}{\Gamma\left(\frac{s}{2}\right)}
\]

\[
= \frac{2^{s-1}}{\sqrt{\pi}} \Gamma\left(\frac{s}{2}\right) \Gamma\left(\frac{1+s}{2}\right) / \Gamma(s) \cdot \Lambda(1-s) / \Lambda(s)
\]

\[= 1.\]
Theorem (Leonhard Euler)

Let $B_n$ denote the $n$th Bernoulli number, that is, that rational number which appears in the power series expansion

$$\frac{t}{e^t - 1} = \sum_{n=1}^{\infty} B_n \frac{t^n}{n!} = 1 + \left(-\frac{1}{2}\right)t + \left(+\frac{1}{6}\right)\frac{t^2}{2} + \left(-\frac{1}{30}\right)\frac{t^4}{24} + \cdots.$$ 

- $\zeta(-n) = -\frac{B_{n+1}}{n+1}$ is a rational number when evaluated at any negative integer.
- $\zeta(-2k) = 0$ at the negative even integers.
- $\zeta(2k) = \frac{(-1)^{k+1}B_{2k}}{2(2k)!} (2\pi)^{2k}$ at the positive even integers.

The negative even integers are called the trivial zeros of the Riemann zeta function. The Riemann Hypothesis asserts that if $\zeta(s) = 0$ then either (1) $s = -2k$ is a negative even integer, or (2) $\text{Re}(s) = 1/2$. 

Proof

We show the second statement. Consider the function equation

$$
\zeta(1 - s) = \frac{2}{(2 \pi)^s} \cos\left(\frac{\pi s}{2}\right) \Gamma(s) \zeta(s), \quad 0 < \Re(s) < 1.
$$

Any meromorphic continuation of $\zeta(s)$ to the entire complex plane must satisfy this relation. If we set $s = 2k + 1$, then we have the identity

$$
\zeta(-2k) = -\frac{1}{4^k \pi^{2k+1}} \sin(\pi k) \Gamma(2k+1) \zeta(2k+1)
$$

for $k = 1, 2, 3, \ldots$

$$
= 0
$$

We show the third statement. Let $s = 2k$ be a positive even integer, so that $1 - s = -n$ for $n = 2k - 1$ is a negative odd integer. Then we have

$$
-\frac{B_{2k}}{2k} = \zeta(1 - 2k) = \frac{2}{(2 \pi)^{2k}} \cos\left(\frac{2k \pi}{2}\right) \Gamma(2k) \zeta(2k) = \frac{2(2k - 1)! (-1)^k}{(2 \pi)^{2k}} \zeta(2k).
$$

Solving for $\zeta(2k)$ gives the result.
Corollary

1 + 2 + 3 + 4 + \cdots + n + \cdots = -\frac{1}{12}.

1 + 2^3 + 3^3 + 4^3 + \cdots + n^3 + \cdots = +\frac{1}{120}.

1 + 2^{2k-1} + 3^{2k-1} + 4^{2k-1} + \cdots + n^{2k-1} + \cdots = -\frac{B_{2k}}{2k}.

Since \( \zeta(s) = 1 + 1/2^s + 1/3^s + \cdots + 1/n^s + \cdots \), we find that

\[ 1 + 2 + 3 + 4 + \cdots + n + \cdots = \zeta(-1) = -\frac{1}{12}; \]

\[ 1 + 2^3 + 3^3 + 4^3 + \cdots + n^3 + \cdots = \zeta(-3) = +\frac{1}{120}; \]

\[ 1 + 2^{2k-1} + 3^{2k-1} + 4^{2k-1} + \cdots + n^{2k-1} + \cdots = \zeta(1 - 2k) = -\frac{B_{2k}}{2k}. \]

(But \( \zeta(s) = 1 + 1/2^s + 1/3^s + \cdots + 1/n^s + \cdots \) only makes sense for \( \text{Re}(s) > 1! \))
Proposition (Carl Gustav Jacob Jacobi, 1829)

Denote the function

\[ \Theta(t) = \prod_{m=1}^{\infty} \left( 1 - e^{-2mt^2} \right) \left( 1 + e^{(1-2m)t^2} \right)^2 = 1 + 2 \sum_{n=1}^{\infty} e^{-n^2 t^2}. \]

- \( \Theta(1/t) = t \Theta(t) \) for all \( t > 0 \).
- \( \lim_{t \to \infty} \Theta(t) = 1. \)

Can this be generalized?
\[ \Gamma(1) = SL_2(\mathbb{Z}) \text{ acts on the upper-half plane } \mathbb{H} = \{ z \in \mathbb{C} \mid \text{Im}(z) > 0 \} \text{ by} \]
\[
\gamma z = \frac{az + b}{cz + d} \quad \text{where} \quad \gamma = \begin{pmatrix} a & b \\ c & d \end{pmatrix}.
\]

**Definitions**

Let \( N \) be a positive integer and \( k \) be a positive even integer.

- \( \Gamma_0(N) = \left\{ \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in SL_2(\mathbb{Z}) \mid c \equiv 0 \text{ mod } N \right\} \).

- A modular form of level \( N \) and weight \( k \) is a function \( f : \mathbb{H} \to \mathbb{C} \) satisfying
  - \( f \) is holomorphic: \( f \) analytic on the upper-half plane;
  - \( f \) is cuspidal: \( \lim_{z \to i\infty} |f(z)| < \infty \); and
  - \( f \) is automorphic: \( f(\gamma z) = (cz + d)^k f(z) \) for \( \gamma \in \Gamma_0(N) \).

\[
\gamma = \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix} \in \Gamma_0(N) \quad \implies \quad f(z + 1) = f(z)
\]
so that each modular form has a \textit{q-series expansion}:

\[
f(z) = \sum_{n \in \mathbb{Z}} a_n e^{2\pi inz} = \sum_{n=0}^{\infty} a_n q^n \quad \text{where} \quad q = e^{2\pi iz}.
\]
Eisenstein Series

**Definitions**

- Let the **divisor function** $\sigma_k(n) = \sum_{d|n} d^k$ be the sum over the $k$th powers of the divisors $d$ of a positive integer $n$.

- Let the **Bernoulli numbers** $B_n$ be defined by the power series expansion

$$\frac{t}{e^t - 1} = \sum_{n=1}^{\infty} B_n \frac{t^n}{n!} = 1 + \left( -\frac{1}{2} \right) t + \left( +\frac{1}{6} \right) \frac{t^2}{2} + \left( -\frac{1}{30} \right) \frac{t^4}{24} + \cdots. $$

- For every even integer $k$, denote $E_k(z) = 1 - \frac{2k}{B_k} \sum_{n=1}^{\infty} \sigma_{k-1}(n) q^n$.

**Proposition**

$E_k$ is a modular form of level $N = 1$ and weight $k$. In particular,

- $E_k(\gamma z) = (cz + d)^k E_k(z)$ for $\gamma \in \Gamma(1) = SL_2(\mathbb{Z})$.

- $E_k(-1/z) = z^k E_k(z)$

- $\lim_{z \to i \infty} E_k(z) = 1$
Proposition

Define

\[ E_4(z) = 1 + 240 \sum_{n=1}^{\infty} \sigma_3(n) q^n \quad E_{12}(z) = 1 + \frac{65520}{691} \sum_{n=1}^{\infty} \sigma_{11}(n) q^n \]
\[ E_6(z) = 1 - 504 \sum_{n=1}^{\infty} \sigma_5(n) q^n \quad \Delta(z) = q \prod_{n=1}^{\infty} (1 - q^n)^{24} = \sum_{n=1}^{\infty} \tau(n) q^n \]

- \[ 691 E_{12}(z) = 441 E_4(z)^3 + 250 E_6(z)^2. \]
- \[ 1728 \Delta(z) = E_4(z)^3 - E_6(z)^2. \]
- \[ \Delta(z) \] is a modular form of level \( N = 1 \) and weight \( k = 12 \). In particular,
  - \[ \Delta(-1/z) = z^{12} \Delta(z) \]
  - \[ \lim_{z \to i} \Delta(z) = 0. \]

\( \Delta \) is called the modular discriminant. Any modular form \( f : \mathbb{H} \to \mathbb{C} \) satisfying \( \lim_{z \to i} f(z) = 0 \) is called a cusp form. Denote the collection by \( S_k(\Gamma_0(N)) \).
Application #1: Representing Integers as the Sums of Squares
Generating Functions, Partitions, and $q$-Series
Modular Forms
Applications

Representing Integers as the Sums of Squares
Ramanujan Tau Function
Elliptic Curves and the Taniyama-Shimura-Weil Conjecture

Adrien-Marie Legendre
September 18, 1752 – January 10, 1833
### Legendre’s Four-Square Theorem

**Theorem (Adrien-Marie Legendre, 1797-8)**

*Every natural number* \( n \) *can be written as the sum of at most four squares.*

<table>
<thead>
<tr>
<th>( n )</th>
<th>Expression</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>( 1^2 + 0^2 + 0^2 + 0^2 )</td>
</tr>
<tr>
<td>2</td>
<td>( 1^2 + 1^2 + 0^2 + 0^2 )</td>
</tr>
<tr>
<td>3</td>
<td>( 1^2 + 1^2 + 1^2 + 0^2 )</td>
</tr>
<tr>
<td>4</td>
<td>( 2^2 + 0^2 + 0^2 + 0^2 )</td>
</tr>
<tr>
<td>5</td>
<td>( 2^2 + 1^2 + 0^2 + 0^2 )</td>
</tr>
<tr>
<td>6</td>
<td>( 2^2 + 1^2 + 1^2 + 0^2 )</td>
</tr>
<tr>
<td>7</td>
<td>( 2^2 + 1^2 + 1^2 + 1^2 )</td>
</tr>
<tr>
<td>8</td>
<td>( 2^2 + 2^2 + 0^2 + 0^2 )</td>
</tr>
<tr>
<td>9</td>
<td>( 3^2 + 0^2 + 0^2 + 0^2 )</td>
</tr>
<tr>
<td>10</td>
<td>( 3^2 + 1^2 + 0^2 + 0^2 )</td>
</tr>
<tr>
<td>11</td>
<td>( 3^2 + 1^2 + 1^2 + 0^2 )</td>
</tr>
<tr>
<td>12</td>
<td>( 2^2 + 2^2 + 2^2 + 0^2 )</td>
</tr>
<tr>
<td>13</td>
<td>( 3^2 + 2^2 + 0^2 + 0^2 )</td>
</tr>
<tr>
<td>14</td>
<td>( 3^2 + 2^2 + 1^2 + 0^2 )</td>
</tr>
<tr>
<td>15</td>
<td>( 3^2 + 2^2 + 1^2 + 1^2 )</td>
</tr>
<tr>
<td>16</td>
<td>( 4^2 + 4^2 + 0^2 + 0^2 )</td>
</tr>
<tr>
<td>17</td>
<td>( 4^2 + 4^2 + 1^2 + 0^2 )</td>
</tr>
<tr>
<td>18</td>
<td>( 3^2 + 3^2 + 0^2 + 0^2 )</td>
</tr>
<tr>
<td>19</td>
<td>( 3^2 + 3^2 + 1^2 + 0^2 )</td>
</tr>
<tr>
<td>20</td>
<td>( 4^2 + 2^2 + 0^2 + 0^2 )</td>
</tr>
<tr>
<td>21</td>
<td>( 4^2 + 2^2 + 1^2 + 0^2 )</td>
</tr>
<tr>
<td>22</td>
<td>( 3^2 + 3^2 + 2^2 + 0^2 )</td>
</tr>
<tr>
<td>23</td>
<td>( 3^2 + 3^2 + 2^2 + 1^2 )</td>
</tr>
<tr>
<td>24</td>
<td>( 4^2 + 2^2 + 2^2 + 0^2 )</td>
</tr>
<tr>
<td>25</td>
<td>( 5^2 + 0^2 + 0^2 + 0^2 )</td>
</tr>
<tr>
<td>26</td>
<td>( 5^2 + 1^2 + 0^2 + 0^2 )</td>
</tr>
<tr>
<td>27</td>
<td>( 3^2 + 3^2 + 3^2 + 0^2 )</td>
</tr>
<tr>
<td>28</td>
<td>( 5^2 + 1^2 + 1^2 + 1^2 )</td>
</tr>
<tr>
<td>29</td>
<td>( 5^2 + 2^2 + 0^2 + 0^2 )</td>
</tr>
<tr>
<td>30</td>
<td>( 5^2 + 2^2 + 1^2 + 0^2 )</td>
</tr>
</tbody>
</table>

*https://en.wikipedia.org/wiki/Lagrange’s_four-square_theorem*
Carl Gustav Jacob Jacobi

December 10, 1804 – February 18, 1851

https://en.wikipedia.org/wiki/Carl_Gustav_Jacob_Jacobi
Recall that we considered the function

\[ \Theta(t) = \prod_{m=1}^{\infty} \left( 1 - q^{2m} \right) \left( 1 + q^{2m-1} \right)^2 = 1 + 2 \sum_{n=1}^{\infty} q^{n^2}, \quad q = e^{-\pi t^2}. \]

**Theorem (Carl Gustav Jacob Jacobi, 1834)**

*For each natural number \( m \), define the function*

\[ \theta_m(q) = \left( \sum_{n \in \mathbb{Z}} q^{n^2} \right)^m = \sum_{n=1}^{\infty} r_m(n) q^n. \]

- \( r_m(n) \) counts the number of ways a natural number \( n = n_1^2 + n_2^2 + \cdots + n_m^2 \)
  can be written as the sum of \( m \) squares \( n_i^2 \).

- \( \theta_4(q) = \left( \sum_{n \in \mathbb{Z}} q^{n^2} \right)^4 = 1 + 8 \left( \sum_{n=1}^{\infty} \frac{n q^n}{1 - q^n} - \sum_{n=1}^{\infty} \frac{4 n q^{4n}}{1 - q^{4n}} \right). \)

- Say \( m \geq 4 \). Then \( r_m(n) \geq 8 \left( \sum_{d|n} d - \sum_{4d|n} d \right) \). In particular, \( r_m(n) \neq 0 \).

[https://en.wikipedia.org/wiki/Jacobi%27s_four-square_theorem](https://en.wikipedia.org/wiki/Jacobi%27s_four-square_theorem)
Application #2:
Congruences with the Ramanujan Tau Function
Generating Functions, Partitions, and $q$-Series
Modular Forms
Applications

Representing Integers as the Sums of Squares
Ramanujan Tau Function
Elliptic Curves and the Taniyama-Shimura-Weil Conjecture

Srinivasa Ramanujan Iyengar
December 22, 1887 – April 26, 1920

Ramanujan Tau Function

$$\Delta(z) = q \cdot \prod_{n=1}^{\infty} (1 - q^n)^2 = \sum_{n=1}^{\infty} \tau(n) q^n$$

where

$$q = e^{2\pi i z}.$$

<table>
<thead>
<tr>
<th>$n$</th>
<th>$\tau(n)$</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>1</td>
</tr>
<tr>
<td>2</td>
<td>-24</td>
</tr>
<tr>
<td>3</td>
<td>252</td>
</tr>
<tr>
<td>4</td>
<td>-1472</td>
</tr>
<tr>
<td>5</td>
<td>4830</td>
</tr>
<tr>
<td>6</td>
<td>-6048</td>
</tr>
<tr>
<td>7</td>
<td>-16744</td>
</tr>
<tr>
<td>8</td>
<td>84480</td>
</tr>
<tr>
<td>9</td>
<td>-113643</td>
</tr>
<tr>
<td>10</td>
<td>-115920</td>
</tr>
<tr>
<td>11</td>
<td>534612</td>
</tr>
<tr>
<td>12</td>
<td>-370944</td>
</tr>
<tr>
<td>13</td>
<td>-577738</td>
</tr>
<tr>
<td>14</td>
<td>401856</td>
</tr>
<tr>
<td>15</td>
<td>1217160</td>
</tr>
<tr>
<td>16</td>
<td>987136</td>
</tr>
</tbody>
</table>

**Proposition**

- $\tau(n) \equiv \sigma_{11}(n) \pmod{2^{11}}$ whenever $n \equiv 1 \pmod{8}$.
- $\tau(n) \equiv 1217 \sigma_{11}(n) \pmod{2^{13}}$ whenever $n \equiv 3 \pmod{8}$.
- $\tau(n) \equiv 1537 \sigma_{11}(n) \pmod{2^{12}}$ whenever $n \equiv 5 \pmod{8}$.
- $\tau(n) \equiv 705 \sigma_{11}(n) \pmod{2^{14}}$ whenever $n \equiv 7 \pmod{8}$.

https://en.wikipedia.org/wiki/Ramanujan_tau_function
Proposition

Define

\[
E_4(z) = 1 + 240 \sum_{n=1}^{\infty} \sigma_3(n) q^n \quad E_{12}(z) = 1 + \frac{65520}{691} \sum_{n=1}^{\infty} \sigma_{11}(n) q^n \\
E_6(z) = 1 - 504 \sum_{n=1}^{\infty} \sigma_5(n) q^n \quad \Delta(z) = q \prod_{n=1}^{\infty} (1 - q^n)^{24} = \sum_{n=1}^{\infty} \tau(n) q^n
\]

- $691 E_{12}(z) = 441 E_4(z)^3 + 250 E_6(z)^2$.
- $1728 \Delta(z) = E_4(z)^3 - E_6(z)^2$.
- $\Delta(z)$ is a modular form of level $N = 1$ and weight $k = 12$. In particular,
  - $\Delta(-1/z) = z^{12} \Delta(z)$
  - $\lim_{z \to i} \Delta(z) = 0$.

$\Delta$ is called the **modular discriminant**. Any modular form $f : \mathbb{H} \to \mathbb{C}$ satisfying $\lim_{z \to i} f(z) = 0$ is called a **cusp form**. Denote the collection by $S_k(\Gamma_0(N))$. 

---

MA 59800-614-27988: Classical Modular Forms

An Introduction to Classical Modular Forms
Let the divisor function \( \sigma_k(n) = \sum_{d|n} d^k \) be the sum over the \( k \)th powers of the divisors \( d \) of a positive integer \( n \).

**Proposition (Srinivasa Ramanujan, 1916)**

\[ \tau(n) \equiv \sigma_{11}(n) \mod 691 \] for all natural numbers \( n \).

Since \( p = 691 \) appears in the numerator of \( B_{12} \), this gives the congruence

\[
691 + 65520 \left[ \sum_{n=1}^{\infty} \sigma_{11}(n) q^n \right] = 691 E_{12}(z)
\]

\[
= 441 E_4(z)^3 + 250 E_6(z)^2
\]

\[
\equiv 441 \cdot [E_4(z)^3 - E_6(z)^2] \mod 691
\]

\[
\equiv 65520 \Delta(z) \mod 691.
\]

**Conjecture**

\( \tau(n) \neq 0 \) for all natural numbers \( n \).
Application #3:
Elliptic Curves and the Taniyama-Shimura-Weil Conjecture
Godfrey Harold Hardy
February 7, 1877 – December 1, 1947
I remember once going to see [Srinivasa Ramanujan] when he was lying ill at Putney. I had ridden in taxi-cab No. 1729, and remarked that the number seemed to be rather a dull one, and that I hoped it was not an unfavourable omen. “No”, he replied, “it is a very interesting number; it is the smallest number expressible as the sum of two [positive] cubes in two different ways.” – Godfrey Harold Hardy, 1919

Definition

The $n$th taxicab number $N = \text{Taxicab}(n)$ is defined as the least natural number which can be expressed as a sum of two positive cubes in $n$ distinct ways.

<table>
<thead>
<tr>
<th>$n$</th>
<th>$N = \text{Taxicab}(n)$</th>
<th>Sum of Cubes</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>2</td>
<td>$1^3 + 1^3$</td>
</tr>
<tr>
<td></td>
<td>1729</td>
<td>$1^3 + 12^3 = 9^3 + 10^3$</td>
</tr>
<tr>
<td>3</td>
<td>87539319</td>
<td>$167^3 + 436^3 = 228^3 + 423^3 = 255^3 + 414^3$</td>
</tr>
<tr>
<td>4</td>
<td>6963472309248</td>
<td>$2421^3 + 19083^3 = \cdots$</td>
</tr>
<tr>
<td>5</td>
<td>48988659276962496</td>
<td>$38787^3 + 365757^3 = \cdots$</td>
</tr>
<tr>
<td>6</td>
<td>24153319581254312065344</td>
<td>$58162^3 + 28906206^3 = \cdots$</td>
</tr>
</tbody>
</table>

https://en.wikipedia.org/wiki/Taxicab_number
Johann Carl Friedrich Gauss
April 30, 1777 – February 23, 1855
Fix an odd prime $p$, and denote the finite field of $p$ elements

$$
\mathbb{F}_p = \mathbb{Z}/p\mathbb{Z} = \{0, 1, 2, \ldots, p-1\}.
$$

**Theorem (Carl Friedrich Gauss, 1798)**

Consider the Fermat curve $\mathcal{F}_3 : a^3 + b^3 = c^3$.

- If either $p = 3$ or $p \equiv 2 \mod 3$, then $\#\mathcal{F}_3(\mathbb{F}_p) = p + 1$.
- If $p \equiv 1 \mod 3$, then there exist integers $a_p$ and $b_p$ such that

$$
\#\mathcal{F}_3(\mathbb{F}_p) = p + 1 - a_p \quad \text{and} \quad 4p = a_p^2 + 27b_p^2.
$$

<table>
<thead>
<tr>
<th>$p$</th>
<th>$#\mathcal{F}_3(\mathbb{F}_p)$</th>
<th>$a_p$</th>
<th>$b_p$</th>
</tr>
</thead>
<tbody>
<tr>
<td>7</td>
<td>9</td>
<td>-1</td>
<td>1</td>
</tr>
<tr>
<td>13</td>
<td>9</td>
<td>5</td>
<td>1</td>
</tr>
<tr>
<td>19</td>
<td>27</td>
<td>-7</td>
<td>1</td>
</tr>
<tr>
<td>31</td>
<td>36</td>
<td>-4</td>
<td>2</td>
</tr>
<tr>
<td>37</td>
<td>27</td>
<td>11</td>
<td>1</td>
</tr>
<tr>
<td>43</td>
<td>36</td>
<td>8</td>
<td>2</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>$p$</th>
<th>$#\mathcal{F}_3(\mathbb{F}_p)$</th>
<th>$a_p$</th>
<th>$b_p$</th>
</tr>
</thead>
<tbody>
<tr>
<td>61</td>
<td>63</td>
<td>-1</td>
<td>3</td>
</tr>
<tr>
<td>67</td>
<td>63</td>
<td>5</td>
<td>3</td>
</tr>
<tr>
<td>73</td>
<td>81</td>
<td>-7</td>
<td>3</td>
</tr>
<tr>
<td>79</td>
<td>63</td>
<td>17</td>
<td>1</td>
</tr>
<tr>
<td>97</td>
<td>117</td>
<td>-19</td>
<td>1</td>
</tr>
<tr>
<td>103</td>
<td>117</td>
<td>-13</td>
<td>3</td>
</tr>
</tbody>
</table>
Proof of Gauss’s Theorem

First assume that \( p \equiv 2 \mod 3 \). We have a bijection

\[
P^1(\mathbb{F}_p) \rightarrow \left\{ (a : b : c) \in P^2(\mathbb{F}_p) \mid a^3 + b^3 = c^3 \right\}
\]

\[\alpha : \beta \mapsto \left( \alpha : \beta : (\alpha^3 + \beta^3)^{(2p-1)/3} \right)\]

Now assume \( p \equiv 1 \mod 3 \). There exists a nontrivial cubic character \( \chi_p : \mathbb{F}_p^\times \rightarrow \mathbb{C}^\times \). Upon setting \( \chi_p(0) = 0 \), define the Gauss sum

\[
\tau(\chi_p) = \sum_{\alpha \in \mathbb{F}_p} \chi_p(\alpha) \zeta_p^\alpha = -e^{i\theta_p/3} \sqrt{p}
\]

for some angle \( \theta_p \). Note that for any \( \alpha \in \mathbb{F}_p \), we have the formula

\[
\# \left\{ a \in \mathbb{F}_p \mid a^3 = \alpha \right\} = 1 + \chi_p(\alpha) + \chi_p(\alpha)^2.
\]
Now define **Jacobi sum** as

\[ J(\chi_p, \chi_p) = \sum_{\alpha+\beta=1} \chi_p(\alpha) \chi_p(\beta) = \frac{\tau(\chi_p)^2}{\tau(\chi_p^2)} = -e^{i\theta_p} \sqrt{p}. \]

Writing \( J(\chi_p, \chi_p) = c_p + d_p \zeta_3 \), we have \( |J(\chi_p, \chi_p)|^2 = c_p^2 - c_p d_p + d_p^2 \).

Choose the rational integers

\[
\begin{align*}
    a_p &= d_p - 2 c_p \\
    b_p &= d_p/3
\end{align*}
\]

\[ \implies \begin{cases} 
    4p = a_p^2 + 27b_p^2 \\
    a_p \equiv 2 \mod 3
\end{cases} \]

Finally, count the number of points:

\[
\# \mathcal{F}_3(\mathbb{F}_p) = 3 + \sum_{\alpha+\beta=1} \# \left\{ a \in \mathbb{F}_p \middle| a^3 = \alpha \right\} \times \# \left\{ b \in \mathbb{F}_p \middle| b^3 = \beta \right\} \\
= p + 1 + J(\chi_p, \chi_p) + J(\chi_p^2, \chi_p^2) \\
= p + 1 - a_p.
\]
Consider the elliptic curve $E: y^2 - y = x^3 - 7$. For all primes $p \neq 3$, 

$$(\sqrt{p} - 1)^2 \leq \#E(\mathbb{F}_p) \leq (\sqrt{p} + 1)^2.$$ 

We have a bijection

$\mathcal{F}_3 : a^3 + b^3 = c^3 \rightarrow E : y^2 - y = x^3 - 7$

$$(a : b : c) \mapsto (3c : -4a + 5b : a + b)$$

Hence

$$p + 1 - \#E(\mathbb{F}_p) = a_p = \begin{cases} 
0 & \text{if } p \equiv 2 \pmod{3}, \\
\pm \sqrt{4p - 27b_p^2} & \text{if } p \equiv 1 \pmod{3}.
\end{cases}$$

In either case we have $|p + 1 - \#E(\mathbb{F}_p)| \leq 2\sqrt{p}$. 
Elliptic Curves

Definitions

Consider an equation with coefficients in a field \( F \), say
\[
E : \quad y^2 + a_1 xy + a_3 y = x^3 + a_2 x^2 + a_4 x + a_6.
\]

- If \( F \) has characteristic different from 2 and 3, we may write
\[
E : \quad y^2 = x^3 - \frac{3}{12^2} c_4 x - \frac{2}{12^3} c_6 \quad \text{and} \quad \Delta(E) = \frac{c_4^3 - c_6^2}{12^3}.
\]

We say \( E \) is an elliptic curve defined over \( F \) if \( \Delta(E) \neq 0 \).

- The collection of \( F \)-rational points on \( E \) defined as the set
\[
E(F) = \left\{ (x_1 : x_2 : x_0) \in \mathbb{P}^2(F) \left| \begin{array}{l}
x_2^2 x_0 + a_1 x_1 x_2 x_0 + a_3 x_2^2 x_0 \\
= x_1^3 + a_2 x_1^2 x_0 + a_4 x_1 x_0^2 + a_6 x_0^3
\end{array} \right. \right\}
\]
having a specified base point \( \mathcal{O} = (0 : 1 : 0) \).

- Define the \( j \)-invariant as
\[
j(E) = \frac{c_4^3}{\Delta(E)} = 12^3 \frac{c_4^3}{c_4^3 - c_6^2}.
\]
Taxi Cab Numbers and Elliptic Curves

Definition

The \textit{nth taxicab number} $N = \text{Taxicab}(n)$ is defined as the least natural number which can be expressed as a sum of two positive cubes in $n$ distinct ways.

Proposition

Fix a nonzero integer $N$.

- The curve $a^3 + b^3 = N c^3$ is just the elliptic curve $E : y^2 = x^3 - 432 N^2$ defined over $F = \mathbb{Q}$.
- An expression $N = (a_0/c_0)^3 + (b_0/c_0)^3$ as the sum of two positive cubes corresponds to a $\mathbb{Q}$-rational point $(x_0, y_0)$ on $E$.
- If $N = \text{Taxicab}(n)$ is a taxicab number, then $E : y^2 = x^3 - 432 N^2$ has infinitely many $\mathbb{Q}$-rational points.

We have the bijection

$$\mathcal{F}_3 : \ a^3 + b^3 = N c^3 \quad \rightarrow \quad E : \ y^2 = x^3 - 432 N^2$$

$$(a : b : c) \quad \mapsto \quad (12 N c : 36 N (a - b) : a + b)$$
**Group Law**

**Definition**

Let $P, Q \in E(F)$. Denote $P \ast Q$ as the point of intersection of $E$ and the line through $P$ and $Q$, and denote $P \oplus Q = (P \ast Q) \ast \mathcal{O}$.

**Theorem (Henri Poincaré, 1901)**

Consider an elliptic curve $E$ defined over a field $F$. Then $(E(F), \oplus)$ is abelian group with identity $\mathcal{O} = (0 : 1 : 0)$ and inverses $[-1]P = P \ast \mathcal{O}$.
Taniyama-Shimura-Weil Conjecture

For an even integer $k$, a cusp form of level $N$ and weight $k$ is a function $f : \mathcal{H} \to \mathbb{C}$ that satisfy

- $f$ is holomorphic: $f$ analytic on the upper-half plane;
- $f$ is cuspidal: $\lim_{z \to i \infty} f(z) = 0$; and
- $f$ is automorphic: $f(\gamma z) = (cz + d)^k f(z)$ for $\gamma \in \Gamma_0(N)$.

Denote the collection of such functions by $S_k(\Gamma_0(N))$.

Theorem (Christophe Breuil, Brian Conrad, Fred Diamond, Richard Taylor, and Andrew Wiles; 2001)

Let $E$ be an elliptic curve over $E$. For each natural number $n$, define the integer $a_n$ as follows.

- $a_n = \prod p a_p^{e_p}$ whenever $n = \prod p^{e_p}$ as a product of prime powers.
- When $p$ does not divide $\Delta(E)$, define $a_p^{e_p}$ recursively via the relations

$$a_1 = 1, \quad a_p = p + 1 - \# E(\mathbb{F}_p), \quad a_p^{e+1} - a_p a_p^e + p a_p^{e-1} = 0.$$ 

Then there exists a positive integer $N$, divisible only by the primes dividing $\Delta(E)$, such that $f(z) = \sum_{n=1}^{\infty} a_n q^n$ is a cusp form of level $N$ and weight $k = 2$. 
Example #1

Consider the elliptic curve \( E : \ y^2 + y = x^3 - x^2 - 10x - 20 \), and denote

\[
\#E(\mathbb{F}_p) = 1 + \# \left\{ (x, y) \in \mathbb{F}_p \times \mathbb{F}_p \mid y^2 + y = x^3 - x^2 - 10x - 20 \right\}.
\]

For example, \( \#E(\mathbb{F}_5) = 8 \), \( \#E(\mathbb{F}_7) = 8 \), \( \#E(\mathbb{F}_{11}) = 8 \), and \( \#E(\mathbb{F}_{13}) = 16 \).

Proposition

Consider the following function

\[
f(q) = q \prod_{n=1}^{\infty} (1 - q^n)^2 (1 - q^{11n})^2
\]

\[
= q - 2q^2 - q^3 + 2q^4 + q^5 + 2q^6 - 2q^7 - 2q^9 - 2q^{10} + q^{11} - 2q^{12} + 4q^{13} + 4q^{14} - q^{15} - 4q^{16} - 2q^{17} + 4q^{18} + \cdots
\]

- This is a cusp form of level \( N = 11 \) and weight \( k = 2 \).
- The coefficient of \( q^p \) is \( a_p = p + 1 - \#E(\mathbb{F}_p) \).

http://www.lmfdb.org/EllipticCurve/Q/11/a/2
Example #2

Consider the elliptic curve $E : y^2 = x^3 + 5x^2 + 4x$, and denote

$$\# E(\mathbb{F}_p) = 1 + \# \left\{ (x, y) \in \mathbb{F}_p \times \mathbb{F}_p \mid y^2 = x^3 + 5x^2 + 4x \right\}.$$ 

For example, $\# E(\mathbb{F}_5) = 8$, $\# E(\mathbb{F}_7) = 8$, $\# E(\mathbb{F}_{11}) = 8$, and $\# E(\mathbb{F}_{13}) = 16$.

Proposition

Consider the following function

$$f(q) = q \prod_{n=1}^{\infty} \left( 1 - q^{2n} \right) \left( 1 - q^{4n} \right) \left( 1 - q^{6n} \right) \left( 1 - q^{12n} \right)$$

$$= q - q^3 - 2q^5 + q^9 + 4q^{11} - 2q^{13} + 2q^{15} + 2q^{17} - 4q^{19}$$

$$- 8q^{23} - q^{25} - q^{27} + 6q^{29} + 8q^{31} - 4q^{33} + 6q^{37} + 2q^{39}$$

$$- 6q^{41} + 4q^{43} - 2q^{45} - 7q^{49} - 2q^{51} - 2q^{53} - 8q^{55} + 4q^{57} + \cdots$$

- This is a cusp form of level $N = 24$ and weight $k = 2$.
- The coefficient of $q^p$ is $a_p = p + 1 - \# E(\mathbb{F}_p)$.

http://www.lmfdb.org/EllipticCurve/Q/24/a/4
Example #3

Consider the elliptic curve $E : y^2 = x^3 - x$, and denote

$$
\#E(\mathbb{F}_p) = 1 + \# \left\{ (x, y) \in \mathbb{F}_p \times \mathbb{F}_p \mid y^2 = x^3 - x \right\}.
$$

For example, $\#E(\mathbb{F}_3) = 4$, $\#E(\mathbb{F}_5) = 8$, $\#E(\mathbb{F}_7) = 8$, and $\#E(\mathbb{F}_11) = 12$.

Proposition

Consider the following function

$$
f(q) = q \prod_{n=1}^{\infty} \left( 1 - q^{4n} \right)^2 \left( 1 - q^{8n} \right)^2
$$

$$
= q - 2q^5 - 3q^9 + 6q^{13} + 2q^{17} - q^{25} - 10q^{29} - 2q^{37}
$$

$$
+ 10q^{41} + 6q^{45} - 7q^{49} + 14q^{53} - 10q^{61} - 12q^{65} - 6q^{73} + \cdots
$$

- This is a cusp form of level $N = 32$ and weight $k = 2$.
- The coefficient of $q^p$ is $a_p = p + 1 - \#E(\mathbb{F}_p)$.
- If $p \equiv 3 \pmod{4}$ then $a_p = 0$. If $p \equiv 1 \pmod{4}$ then $a_p$ is divisible 2.
Fermat’s Last Theorem

Theorem (Pierre de Fermat, 1670; Andrew Wiles, 1993)

Let \( n \geq 3 \) be an integer. If \( a, b, \) and \( c \) are integers satisfying \( a^n + b^n = c^n \), then \( a \, b \, c = 0 \).

https://en.wikipedia.org/wiki/Fermats_Last_Theorem

Assume that there are nonzero integers \( a, b, \) and \( c \) such that \( a^n + b^n = c^n \).

- Say that \( n \) has no odd prime divisors. Then \( x = c^{n/4}, y = b^{n/4}, \) and \( z = a^{n/2} \) are nonzero integers such that \( x^4 - y^4 = z^2 \). In 1670, Pierre de Fermat showed no such integers exist.

- Say that \( n \) has an odd prime divisor \( \ell \). Then \( A = a^{n/\ell}, B = b^{n/\ell}, \) and \( C = c^{n/\ell} \) are nonzero integers such that \( A^\ell + B^\ell = C^\ell \). Gerhard Frey suggested in 1984 to consider the curve \( E : y^2 = x(x - A^\ell)(x + B^\ell) \) with discriminant \( \Delta(E) = 16 (A \, B \, C)^{2\ell} \). In 1993, Andrew Wiles proved that such an elliptic curve \( E \) must be modular. In 1986, Kenneth Ribet showed that its level must be \( N = 2 \). A simple computation shows that there are no cusp forms of level \( N = 2 \) and weight \( k = 2 \).
Generating Functions, Partitions, and $q$-Series
Modular Forms
Applications

Representing Integers as the Sums of Squares
Ramanujan Tau Function
Elliptic Curves and the Taniyama-Shimura-Weil Conjecture

The Man Who Knew Infinity
Official Theatrical Release Date: April 29, 2016

https://www.youtube.com/watch?v=oXGm9V1fx4w