The Pentagonal Number Theorem and Modular Forms

Tri Nguyen

March 26, 2025

Outline

Warm-up problem

Given a positive number n, how many ways can be write n in the form

$$a_1 + a_2 + \ldots + a_k?$$

Warm - up problem

There are in total 2^{n-1} of them, however, there are a lot of repetitions.

n	1	2	3

Warm - up problem

There are in total 2^{n-1} of them, however, there are a lot of repetitions.

n	1	2	3
	1	2	3
		1+1	1+2
			2+1
			1+1+1

Table: 1

Warm - up problem

There are in total 2^{n-1} of them, however, there are a lot of repetitions.

n	1	2	3

Warm - up problem

There are in total 2^{n-1} of them, however, there are a lot of repetitions.

n	1	2	3
	1	2	3
		1+1	1+2
			2+1
			1+1+1

Table: 1

Warm - up problem

There are in total 2^{n-1} of them, however, there are a lot of repetitions.

n	1	2	3
	1	2	3
		1+1	1+2
			2+1
			1+1+1

Table: 1

So you will get more and more repetitions listing this way. For example

$$\begin{aligned} 4 &= 1+1+1+1 \\ &= 2+1+1 = 1+2+1 = 1+1+2 \\ &= 2+2 \\ &= 3+1 = 1+3 \end{aligned}$$

Partition

We don't want to over-count the number of "partitions", so we will just restrict ourselves to just the way to can write the number of sum of positive integers, up to permutation.

Partition

We don't want to over-count the number of "partitions", so we will just restrict ourselves to just the way to can write the number of sum of positive integers, up to permutation.

Partition

Given a positive integer n, we call a *partition* of n is a representation of n into sum of positive integers, not taking into account of orders. We will denote the number of partition of n by $p(n)$.

Partition

We don't want to over-count the number of "partitions", so we will just restrict ourselves to just the way to can write the number of sum of positive integers, up to permutation.

Partition

Given a positive integer n, we call a *partition* of n is a representation of n into sum of positive integers, not taking into account of orders. We will denote the number of partition of n by $p(n)$.

So in the above examples, we have a few first values of $p(n)$.

n	1	2	3	4	5	6

We don't want to over-count the number of "partitions", so we will just restrict ourselves to just the way to can write the number of sum of positive integers, up to permutation.

Partition

Given a positive integer n, we call a *partition* of n is a representation of n into sum of positive integers, not taking into account of orders. We will denote the number of partition of n by $p(n)$.

So in the above examples, we have a few first values of $p(n)$.

n	1	2	3	4	5	6
$p(n)$	1	2	3	5	7	12

Table: A first few value

Euler's first formulae

Euler came up with the following generating function for $p(n)$

Theorem 1

We have the following identity

$$(1+x+x^2+\dots)(1+x^2+x^4+\dots)(1+x^3+x^6+\dots)(\dots) = \sum p(n)x^n$$

Proof.

This is just combinatorics, we actually counts the number smaller than n that appears the partition. $\square$

A similar method can be used to count the number of partitions that contains a specific set of given number.

Problems?

This method is very slow if one wants to compute $p(n)$ explicitly for n larges.
A programme in *Mathematica* following this method takes around 50s to compute the first fifty values of $p(n)$.

A faster method

Ring of formal series

Let

$$\mathfrak{U} = \left\{ 1 + a_1 x + a_2 x^2 + \ldots = \sum_{\geq 0} a_n x^n \right\}$$

Then we can define a multiplication by

$$(1 + a_1 x + a_2 x^2 + \ldots)(1 + b_1 x + b_2 x^2 + \ldots) = 1 + c_1 x + c_2 x^2 + \ldots$$

where $c_k = a_k + a_{k-1} b_1 + \ldots + b_k$

A faster method

Theorem 2

The set $\mathfrak{U}$ with this product forms a group.

Proof.

Left to the audiences =)). $\square$

In particular, we have that

$$\frac{1}{1-x^k} = \sum_{n\geq 0} x^{nk} = 1 + x^k + x^{2k} + \dots$$

A faster method

Theorem 3

We have the following generating function for $p(n)$

$$\frac{1}{\prod_{k\geq 1}(1-x^k)} = \sum_{n\geq 1} p(n)x^n$$

A faster method

Theorem 3

We have the following generating function for $p(n)$

$$\frac{1}{\prod_{k\geq 1}(1-x^k)} = \sum_{n\geq 1} p(n)x^n$$

Proof.

This follows from theorem 1 by taking the inverses of the series on the left hand sides. $\square$

The pentagonal number theorem

Euler hoped to find a pattern that emerges from the denominator on the left hand side. He did that by multiplying everything and get the following

$$\prod_{k\geq 1}(1-x^k) = 1 - x - x^2 + x^5 + x^7 - x^{12} - x^{15} + x^{22} + x^{26} - x^{35} - x^{40} + \dots$$

The pentagonal number theorem

Euler hoped to find a pattern that emerges from the denominator on the left hand side. He did that by multiplying everything and get the following

$$\prod_{k\geq 1}(1-x^k) = 1 - x - x^2 + x^5 + x^7 - x^{12} - x^{15} + x^{22} + x^{26} - x^{35} - x^{40} + \dots$$

Note that we obviously have

$$(1 - x - x^2 + x^5 + x^7 - x^{12} - \dots)(1 + p(1)x + p(2)x^2 + p(3)x^3 + \dots) = 1$$

The pentagonal number theorem

Euler hoped to find a pattern that emerges from the denominator on the left hand side. He did that by multiplying everything and get the following

$$\prod_{k\geq 1}(1-x^k) = 1 - x - x^2 + x^5 + x^7 - x^{12} - x^{15} + x^{22} + x^{26} - x^{35} - x^{40} + \dots$$

Note that we obviously have

$$(1 - x - x^2 + x^5 + x^7 - x^{12} - \dots)(1 + p(1)x + p(2)x^2 + p(3)x^3 + \dots) = 1$$

So we have a recurrence relation

$$p(n) - p(n-1) - p(n-2) + p(n-5) + p(n-7) - p(n-12) - p(n-15) + \dots = 0$$

Using this relation, it is much faster to compute the partition number.

Why Pentagonal?

If you list the exponents, you get a sequence of number

$$1, 2, 5, 7, 12, 15, 22, 26, 35, 40, \ldots$$

Why Pentagonal?

If you list the exponents, you get a sequence of number

$$1, 2, 5, 7, 12, 15, 22, 26, 35, 40, \ldots$$

The subsequence of number at the odd positions is

$$1, 5, 12, 22, 35, \ldots$$

Why Pentagonal?

If you list the exponents, you get a sequence of number

$$1, 2, 5, 7, 12, 15, 22, 26, 35, 40, \ldots$$

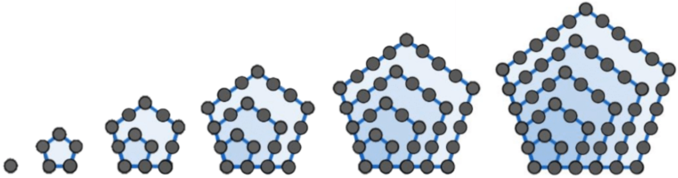
The subsequence of number at the odd positions is

$$1, 5, 12, 22, 35, \ldots$$

All the terms showed up here are the pentagonal number! In particular, they are given by the formulae

$$n = \frac{k(3k-1)}{2}, \quad k \geq 1$$

Why Pentagonal



Pentagonal number theorem

It turns our that the numbers at even positions is also given by pentagonal number formula, with oppositive sig

$$n = \frac{k(3k+1)}{2}, \quad -k \geq 1$$

So Euler conjectured that

Pentagonal Number theorem

$$\prod_{k\geq 1}(1-x^k) = \sum_{k=-\infty}^{\infty} (-1)^k x^{\frac{k(3k-1)}{2}}$$

Pentagonal number theorem

It turns our that the numbers at even positions is also given by pentagonal number formula, with oppositive sig

$$n = \frac{k(3k+1)}{2}, \quad -k \geq 1$$

So Euler conjectured that

Pentagonal Number theorem

$$\prod_{k \geq 1} (1 - x^k) = \sum_{k=-\infty}^{\infty} (-1)^k x^{\frac{k(3k-1)}{2}}$$

This is later proved algebraically by Euler in 1750 and again by Franklin in 1881.

Length of ellipse

We start with an old problem: *How can we compute the perimeter of an ellipse?*

Length of ellipse

We start with an old problem: *How can we compute the perimeter of an ellipse?* We consider the ellipse of the form

$$\frac{x^2}{a^2} + \frac{y^2}{b^2} = 1$$

We know from calculus that the total length can be computed by

$$\int \sqrt{(dx)^2 + (dy)^2} = \sqrt{1 + \left(\frac{dy}{dx}\right)^2} dx$$

Length of an ellipse

Solve for the equation of ellipse in term of y, we get

$$y = b\sqrt{1 - \frac{x^2}{a^2}}$$

which implies that the total length of an ellipse is

$$4a\int_0^1 \sqrt{\frac{1-k^2t^2}{1-t^2}}dt = 4\int_0^1 \frac{1-k^2t^2}{\sqrt{(1-t^2)(1-k^2t^2)}}dt$$

Length of an ellipse

Solve for the equation of ellipse in term of y, we get

$$y = b\sqrt{1 - \frac{x^2}{a^2}}$$

which implies that the total length of an ellipse is

$$4a\int_0^1 \sqrt{\frac{1-k^2t^2}{1-t^2}}dt = 4\int_0^1 \frac{1-k^2t^2}{\sqrt{(1-t^2)(1-k^2t^2)}}dt$$

For $k = 0$, this is just the perimeter of the circle. The general case is called *elliptic integral*.

A case study of Gauss

Gauss essentially tried to compute the elliptic integral by looking at the following integral

$$F(x) = \int_0^x \frac{1}{\sqrt{1-z^4}} dz$$

Mimicking the case for the integral

$$\int_0^x \frac{1}{\sqrt{1-z^2}} dz = \sin^{-1}(x)$$

Gauss tried to find an inverse function of F. This inversion is called *elliptic functions*.

Weierstrass $\wp$ functions

Abel, and later Weierstrass, created an elliptic functions from scratch using the lattice.

Lattice

A lattice $L \subset \mathbb{R}^2$ is a set of the form

$$L = \mathbb{Z}e_1 \oplus \mathbb{Z}e_2$$

where e_1, e_2 are linearly independent over $\mathbb{R}$.

Weierstrass $\wp$ functions

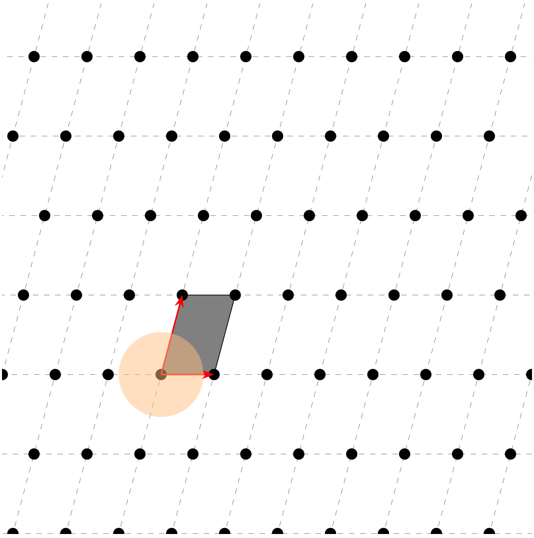


Figure: Example of a lattice

Weierstrass $\wp$ functions

Weierstrass defined his function as

$$\wp(z) = \frac{1}{z^2} + \sum_{m,n\neq 0}\left(\frac{1}{(z - m\omega_1 - n\omega_2)^2} - \frac{1}{(m\omega_1 + n\omega_2)^2}\right)$$

This function is holomorphic and doubly periodic.

Weierstrass $\wp$ functions

Weierstrass defined his function as

$$\wp(z) = \frac{1}{z^2} + \sum_{m,n \neq 0} \left(\frac{1}{(z - m\omega_1 - n\omega_2)^2} - \frac{1}{(m\omega_1 + n\omega_2)^2} \right)$$

This function is holomorphic and doubly periodic. Differentiating both sides yields another elliptic functions

$$\wp'(z) = -2 \sum_{m,n} \frac{1}{(z - m\omega_1 - n\omega_2)^3}$$

Theorem : Doubly periodic functions with prescribed periods

Every doubly periodic function with periods ω_1, ω_2 can be written uniquely in the form

$$R_1(\wp(z)) + R_2(\wp(z))\wp'(z).$$

In other words, any doubly periodic function with periods ω_i is an element of the function field $\mathbb{C}(\wp, \wp')$

In particular, there are not many double periodic functions.

Weierstrass $\wp$ functions

Theorem

We have

$$(\wp'(z))^2 = 4\wp(z)^3 - g_2\wp(z) - g_3$$

Classification of lattices

Starting with the problem on the arc length of ellipse, we come up with the notion of lattices and elliptic functions. Do we know all the possible "lattice shape"?

Classification of lattices

Starting with the problem on the arc length of ellipse, we come up with the notion of lattices and elliptic functions. Do we know all the possible "lattice shape"?

Answer: Up to maginifcation, rotation and change of basis, the answer is yes.

Fundamental domain

Up to rorations and magnifications, we can reduce a lattice

$$L = \mathbb{Z}\omega_1 \oplus \mathbb{Z}\omega_2$$

to a lattice of the form

$$L_z = \mathbb{Z}z \oplus \mathbb{Z}, \quad \Im(z) > 0$$

So the upper half-plane parametrizes the 2 dimensional lattices.

Classification of unit lattices

The map $z \mapsto \mathbb{Z}z \oplus \mathbb{Z}$ induces a bijection

$$\mathrm{SL}_2(\mathbb{Z})\backslash\mathbb{H} \cong \{\text{ lattices}\}/\mathbb{C}^\times$$

Fundamental domain

So we reduce to study the space of lattices by looking the action of $SL_2(\mathbb{Z})$ on the upper half plane. Geometrically, the domain is given by

$$\mathfrak{D} = \{z = x + iy \in \mathbb{H} : |z| \geq 1, -1/2 \leq x \leq 1/2\}$$

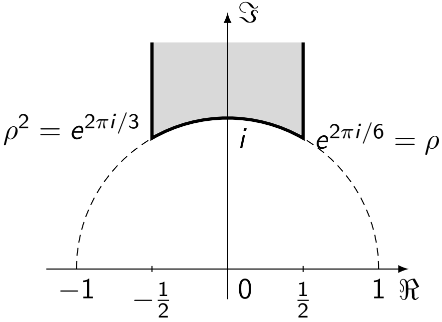
,

Fundamental domain

So we reduce to study the space of lattices by looking the action of $SL_2(\mathbb{Z})$ on the upper half plane. Geometrically, the domain is given by

$$\mathfrak{D} = \{z = x + iy \in \mathbb{H} : |z| \geq 1, -1/2 \leq x \leq 1/2\}$$

,



A brief look at modular forms

Goal: we have to assign each point $z \in \mathfrak{D}$ a number $j(z)$ such that j detects the z corresponding to distinct lattices.

A brief look at modular forms

Goal: we have to assign each point $z \in \mathfrak{D}$ a number $j(z)$ such that j detects the z corresponding to distinct lattices.

Generators of $\mathrm{SL}_2(\mathbb{Z})$

As a group, $\mathrm{SL}_2(\mathbb{Z})$ is generated by two elements

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

A brief look at modular forms

Goal: we have to assign each point $z \in \mathfrak{D}$ a number $j(z)$ such that j detects the z corresponding to distinct lattices.

Generators of $\mathrm{SL}_2(\mathbb{Z})$

As a group, $\mathrm{SL}_2(\mathbb{Z})$ is generated by two elements

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

So we are after a function $j\colon \mathbb{H} \to \mathbb{C}$ such that

$$j(Sz) = j(Tz) = j(z)$$

A brief look at modular forms

If $g(z)$ is a holomorphic function on the unit disk, then $g(e^{2i\pi\tau})$ is a holomorphic function over the upper half plane and have a period $p = 1$. So for each holomophic function on the unit disk, we get a candidate. The problem is to find a function $f(\tau) = g(e^{2i\pi\eta})$ such that

$$f(\tau) = f\left(\frac{1}{-\tau}\right)$$

We have the *Eisenstein series* defined as

$$g_4(\tau) = 60 \sum_{m,n\neq 0} \frac{1}{(m\tau + n)^4}$$

and

$$g_6(\tau) = 140 \sum_{m,n\neq 0} \frac{1}{(m\tau + n)^6}$$

A brief look at modular forms

It can be shown that g_4, g_6 are holomorphic functions over the unit disk. We formalize the notion of modular forms as follows

Definitions of modular forms

A modular form of level k is a function $f(\tau)$ on the upper half plane associated with a power series $g(z)$ by the formula $f(\tau) = g(e^{2i\pi\tau})$ that satisfies

$$f(-1/\tau) = \tau^k f(\tau)$$

We denote M_k the set of such weight k modular forms.

A brief look at modular forms

Theorem

The M_k are finite dimensional vector spaces. When k is odd, they contain only the zero vector.

1. If k is even and $k \equiv 2 \pmod{12}$, then $\dim M_k = \left\lfloor \frac{k}{12} \right\rfloor$.
2. If k is even and $k \not\equiv 2 \pmod{12}$, then $\dim M_k = \left\lfloor \frac{k}{12} \right\rfloor + 1$.
3. Thus $M_0, M_2, M_4, M_6, M_8, M_{10}$, and M_{12} have dimensions $1, 0, 1, 1, 1, 1, 2$.
4. The product of an element of M_k and an element of M_l is an element of M_{k+l}.
5. $g_2 \in M_4$ and $g_3 \in M_6$.
6. M_0 only contains constants.

Remark

We know that over M_{12} we have at least two linearly independent modular forms - denoted by h_1 and h_2. Then

$$j(\tau) = \frac{h_1}{h_2}$$

Seems to be the right function.

Dedekind η function

Now recalled the inverse of the partition generating function discovered by Euler

$$g(z) = 1 - z - z^2 + z^5 + z^7 - z^{12} - z^{15} + \dots$$

This is a holomorphic function over the unit disk. Let $f(\tau) = g(e^{2i\pi\tau})$. Then

Dedekind's theorem

Let $\eta(\tau) = e^{2i\pi\tau/24} f(\tau)$. Then

$$\eta(-1/\tau) = \sqrt{-i\tau}\,\eta(\tau)$$

The $j-$invariant

Let us define

$$j(\tau) = \frac{g_4^2(\tau)}{\eta^{24}(\tau)}$$

Then j has only a pole at ∞ and $j\colon \mathfrak{D} \to \mathbb{C}$ is a bijection.

The $j-$invariant

Let us define

$$j(\tau) = \frac{g_4^2(\tau)}{\eta^{24}(\tau)}$$

Then j has only a pole at ∞ and $j : \mathfrak{D} \to \mathbb{C}$ is a bijection. Therefore we have the following theorem

Main theorem

Two lattices are equivalent under mangnification, rotation, and base change if and only if they have the same $j-$ invariant.