Sum of squares

Lie Fu

University of Strasbourg

15 March, 2024, EES

Question : When can a natural number (=nonnegarive integer) A be written as the sum of two square numbers ?

$$A = n^2 + m^2$$

Definition :
Square number : number of the form n^2.
Examples of square numbers : 0, 1, 4, 9, 16, 25, 36, 49, 64, ...

Examples of sum of two square numbers :
0=0+0, 2=1+1, 4=0+4, 5=1+4, 85=36+49, $2020 = 16^2 + 42^2$...

Examples that are not sums of two square numbers :
3, 7,..., 30,..., 2024, ...

Do experiments

Your turn !

Experiment results :

Numbers that are sums of two squares :

0 ,1, 2, 4, 5, 8, 9, 10, 13, 16, 17, 18, 20, 25, 26, 29, ...

Numbers that are not sums of two squares :

3, 6, 7, 11, 12, 14, 15, 19, 21, 22, 23, 24, 27, 28, 30, ...

Patterns ?

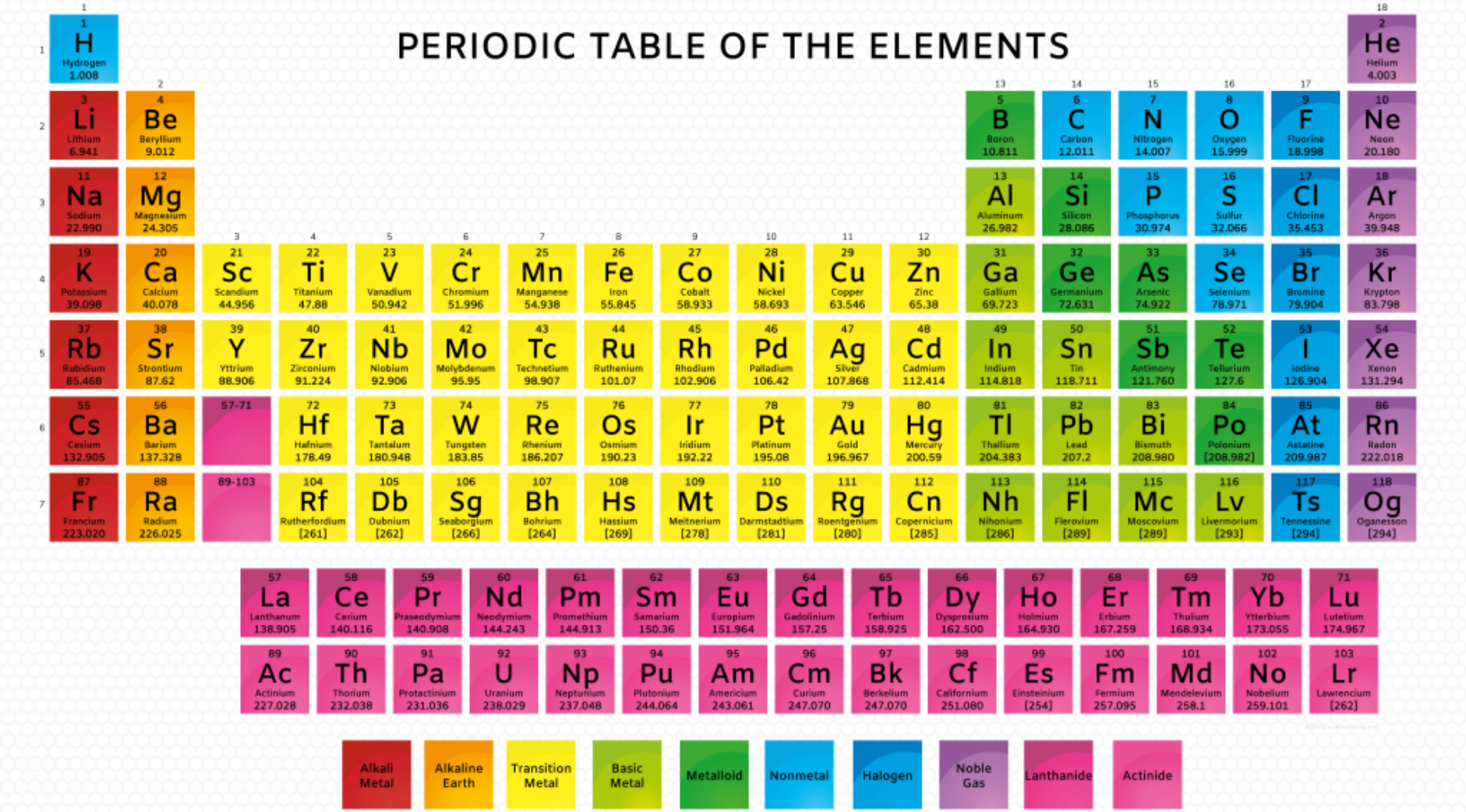
Atoms

Everything is made of atoms.

Ancient Greek word : *Atomos*, meaning "uncuttable".

"If we were to name the most powerful assumption of all, which leads one on and on in an attempt to understand life, it is that all things are made of atoms, and that everything that living things do can be understood in terms of the jigglings and wigglings of atoms."

– Richard P. Feynman, The Feynman Lectures on Physics



Classification of atoms.

"Atoms" for numbers

What are the "atoms" for numbers ?
Answer : **prime numbers**.

Definition A *prime number* is a natural number that cannot be written as a product of two natural numbers > 1.

Examples of prime numbers :
2, 3, 5, 7, 11, 13, 17, 19, 23, 29, 31, 37, 41, 43, 47, 53, 59, 61, 67, 71, 73, 79, 83, 89, 97,... (There are infinitely many !)

Examples of composite numbers :
$4 = 2 \times 2$, $15 = 3 \times 5$, $95 = 5 \times 19$, $2024 = 4 \times 501$ ...

Prime numbers : "atoms" for all natural numbers

Every number is made of prime numbers.

Theorem (Fundamental theorem of arithmetic)

Every natural number (> 1) can be written as a product of powers of distinct prime numbers, in an essentially unique way.

$$n = p_1^{a_1} p_2^{a_2} \cdots p_k^{n_k}.$$

The p_i's are called the *prime factors* of n
The number a_i is called the *multiplicity* of the prime factor p_i
Examples :
$30 = 2 \times 3 \times 5$.
$1200 = 2^4 \times 3 \times 5^2$.
$2024 = 2^3 \times 11 \times 23$

Back to sum of squares

Diophantine equality

$$(a^2 + b^2)(c^2 + d^2) = (ac - bd)^2 + (ad + bc)^2$$

Aside : using complex numbers, this is nothing but $|z_1| \cdot |z_2| = |z_1 \cdot z_2|$.

Consequence : Product of sums of two squares is itself a sum of two squares !

$\Rightarrow$ Only need to consider the prime factors

$\Rightarrow$ Only need to consider the prime factors with *odd* multiplicities.

Experiment results : "atomic" revisit

Numbers that are sums of two squares :

$2,\quad 4=2^2,\quad 5,\quad 8=2^3,\quad 9=3^2,\quad 10=2\times 5,$
$13,\quad 16=2^4,\quad 17,\quad 18=2\times 3^2,\quad 20=2^2\times 5,$
$25=5^2,\quad 26=2\times 13,\quad 29,\ldots$

- **Prime numbers appeared with odd multiplicities :**
  2, 5, 13, 17, 29, ...
- **The missing prime numbers - "bad" primes**
  3, 7, 11, 19, 23, ...

Numbers that are not sums of two squares :

$3,\quad 6=2\times 3,\quad 7,\quad 11,\quad 12=2^2\times 3$
$14=2\times 7,\quad 15=3\times 5,\quad 19,\quad 21=3\times 7,\quad 22=2\times 11$
$23,\quad 24=2^3\times 3,\quad 27=3^3,\quad 28=2^2\times 7,\quad 30=2\times 3\times 5\ldots$

Observation : Each time there is some "bad" prime with odd multiplicity.

Conjecture (= a guess based on evidences and preliminary reasoning) :

- A prime number is bad if it is congruent to 3 modulo 4.
- For a natural number n, if in the (unique) factorization

$$n = p_1^{a_1} p_2^{a_2} p_3^{a_3} \cdots p_k^{a_k}$$

there is no bad prime with odd multiplicity appearing, then n is a sum of two square numbers.

In other words, in order for a number to be sum of two square numbers, it can have some bad primes factors, but each bad prime factor has to appear with pairs.

It's a right guess !

First discovered by Albert Girard in 1625.
Fermat elaborated in a letter to Mersenne (December 25, 1640).

Pierre de Fermat (1607 - 1665)

Marin Mersenne (1588 - 1648)

Fermat's Christmas Theorem of sum of squares

Theorem

A natural number n is the sum of two square numbers if and only if all of its prime factors that are congruent to 3 modulo 4 have even multiplicities.

Examples :

$2024 = 2^3 \times 11 \times 23$, not a sum of two squares.

$2020 = 2^2 \times 5 \times 101$, is a sume of two squares : $2020 = 16^2 + 42^2$.

$21606759720 = 2^3 \times 3^4 \times 5 \times 7^2 \times 13 \times 19^2 \times 29$, is a sum of two squares !

(Challenge : How to find the two square numbers ?)

Proofs

First proof given by L. Euler

Leonhard Euler (1707 - 1783)

- announced in two letters to Goldbach on May 6, 1747 and on April 12, 1749
- Detailed proof published in two articles (between 1752 and 1755).
- Method : infinite descent.

Many more proofs

Joseph-Louis Lagrange (1736 - 1813) Carl Friedrich Gauß (1777 - 1855))

- Proof in 1775, using quadratic forms, later simplified by Gauß in his *Disquisitiones Arithmeticae* (1798).
- Dedekind (two proofs, 1877 & 1894), Heath-Brown (1984), Zagier (one-sentence proof, 1990), Christopher (2016)

Proof for Today

I will present a proof using Minkovski's geometry of numbers, and curiously, π will appear !

Hermann Minkowski (1864 - 1909)

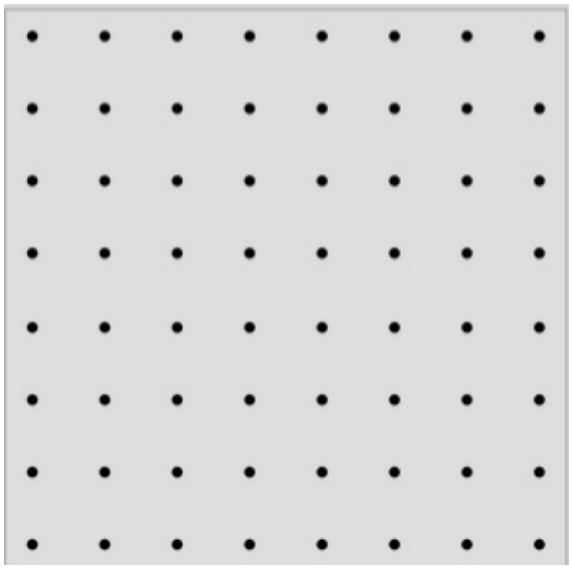
Lattice

Definition : A lattice in the plan is a subset of the form

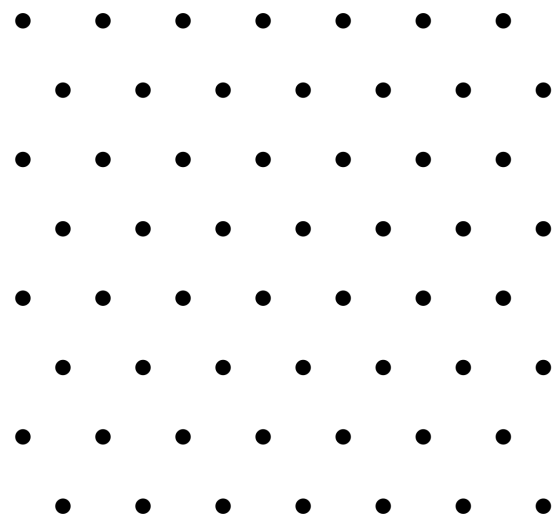
$$\mathbb{L} = \{n\vec{u} + m\vec{v} \mid n, m \text{ integers}\} \subset \mathbb{R}^2,$$

with $\vec{u}, \vec{v}$ are two vectors in the plane.

Examples :



$\vec{u} = (1, 0), \vec{v} = (0, 1)$

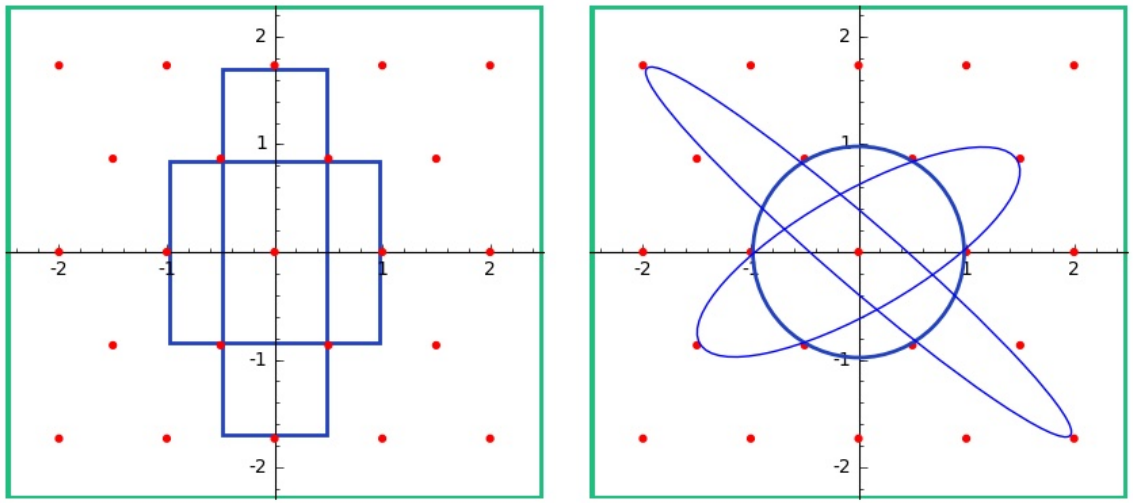


$\vec{u} = (1, 0), \vec{v} = (\frac{-1}{2}, \frac{\sqrt{3}}{2})$

Minkovski theorem : Let T be a *symmetric* and *convex* body in the plan and $\mathbb{L}$ a lattice. If

$$\text{Area}(T) > 4\,\text{Vol}(\mathbb{L}),$$

then T contains a nonzero lattice point of $\mathbb{L}$.



Back to the proof

By Diophantine identity, we are reduced to show :
Goal : Any prime number $p = 4m + 1$ is a sum of two square numbers.

Euler criterion : Let a be a number not divisible by p.
Then a is a square modulo p (that is, $p|m^2 - a$ for some m) if and only if

$$a^{\frac{p-1}{2}} \equiv 1 \mod p.$$

Consequence : If $p - 1$ is divisible by 4, then -1 is a square modulo p.
Hence there is some m such that $p \mid m^2 + 1$

End of Proof : geometry of numbers

Look at the lattice $\mathbb{L}$ in the plane determined by $\vec{u} = (1, m)$ and $\vec{v} = (0, p)$.

$$\mathrm{Vol}(\mathbb{L}) = p.$$

Consider the disc T of radius $r = \sqrt{2p}$, which is symmetric and convex, and

$$\mathrm{Area}(T) = 2\pi p > 4p = 4\,\mathrm{Vol}(\mathbb{L})$$

Minkovski theorem $\Rightarrow$ the disc contains a nonzero lattice point $\vec{w} = (a, b)$. We have

$$0 < ||\vec{w}||^2 < r^2 = 2p.$$

On the other hand, since $p \mid m^2 + 1$,

$$||\vec{w}||^2 = ||x\vec{u} + y\vec{v}||^2 = ||(x, xm + yp)||^2 = x^2(1 + m^2) + p(2xyp + y^2 p)$$

is always divisible by p. The only possibility is

$$a^2 + b^2 = ||\vec{w}||^2 = p$$

More squares ?

Legendre's three-square theorem : A natural number n can be represented as the sum of three square numbers

$$n = x^2 + y^2 + z^2,$$

if and only if n is **not** of the form $n = 4^a(8b + 7)$ for natural numbers a and b.

Question : How many squares do we need to express all natural numbers ?

Lagrange's four square Theorem : Any natural number can be written as the sum of 4 squares.

Joseph-Louis Lagrange (1736 - 1813)

Euler's four-square identity

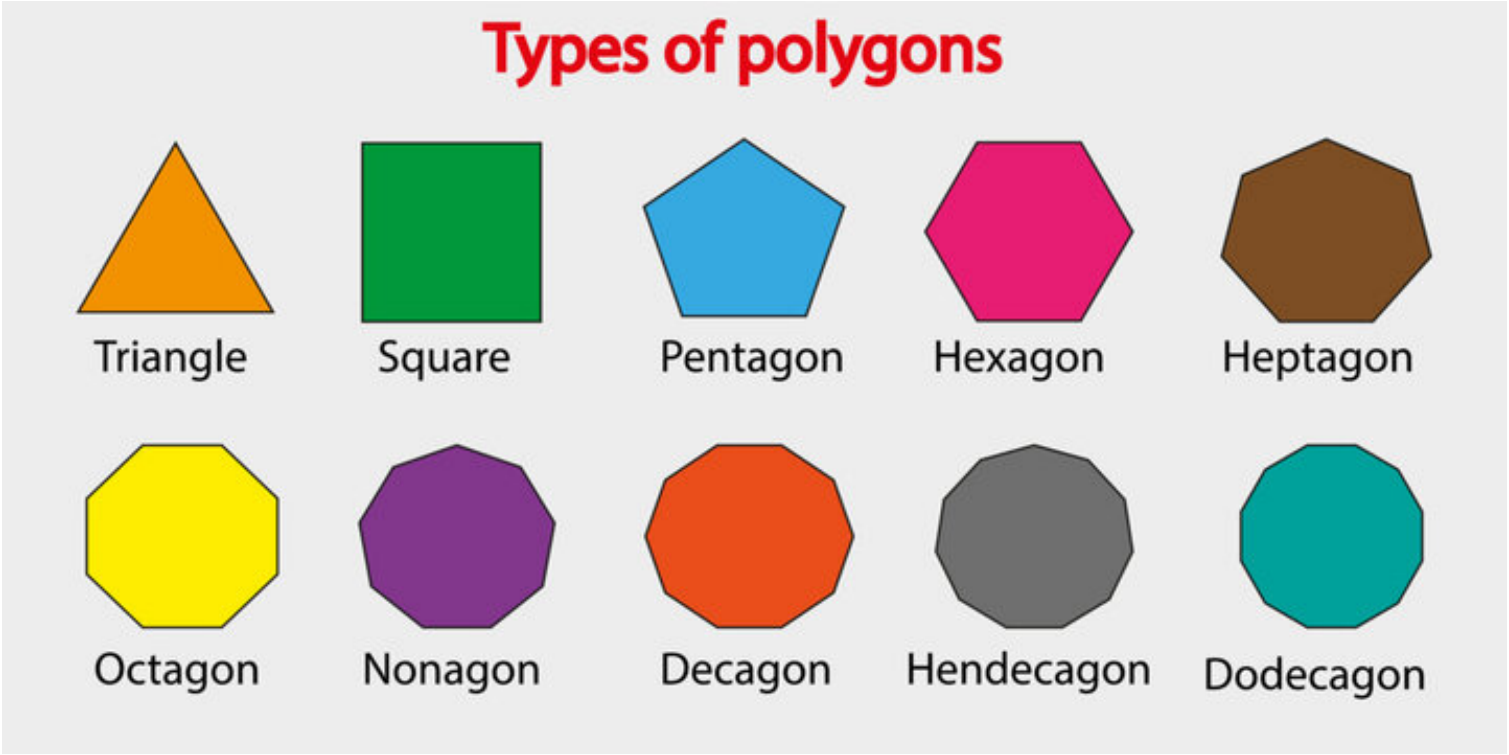
$$(a_1^2 + a_2^2 + a_3^2 + a_4^2)(b_1^2 + b_2^2 + b_3^2 + b_4^2) = (...)^2 + (...)^2 + (...)^2 + (...)^2$$

Consequence : suffices to prove the 4 square theorem for prime numbers.

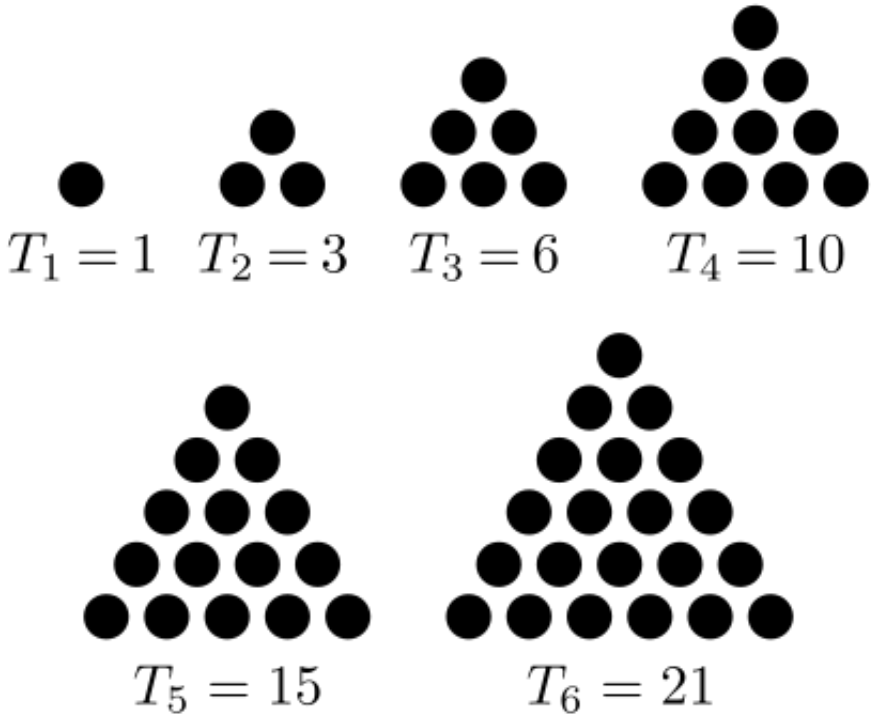
The proof of Lagrange uses infinite descent.

Generalization

Idea : Square $\rightsquigarrow$ (regular) polygons.



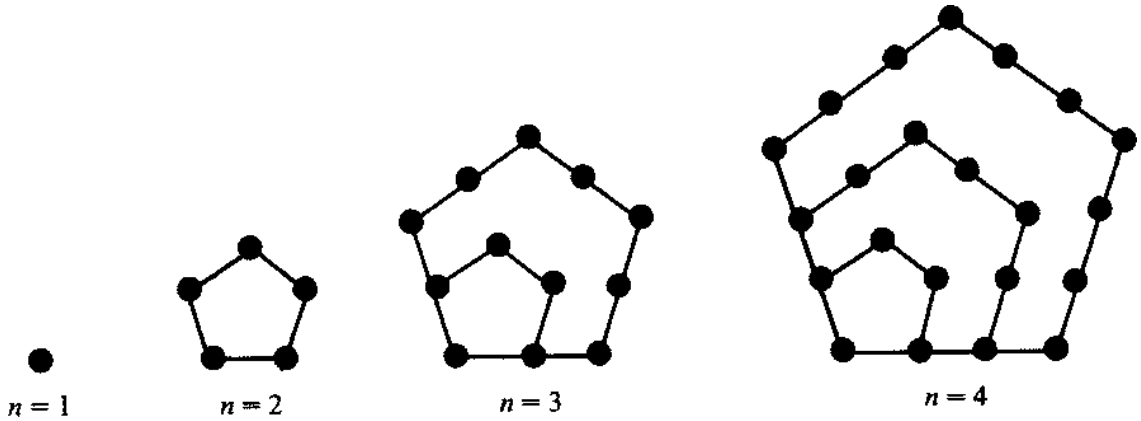
Triangular numbers



Triangular numbers : numbers of the form $\frac{n(n+1)}{2}$

Examples : 0, 1, 3, 6, 10, 15, 21, 28, 36, 45, 55, 66, 78, 91, 105, 120, 136, 153, 171, 190, 210, 231, 253, 276, 300, 325, 351, 378, 406, 435, 465, 496, 528, 561, 595, 630, 666...

Pentagonal numbers



Pentagonal numbers : numbers of the form $\frac{(n+1)(3n+2)}{2}$.
Examples : 0, 1, 5, 12, 22, 35, 51, 70, 92, 117, 145, 176, 210, 247, 287, 330, 376, 425, 477, 532, 590, 651, 715, 782, 852, 925, 1001, 1080, 1162, 1247, 1335,

Fermat's Polygonal Number Theorem

Theorem : Any natural number can be written a sum of n n-gonal numbrers, that is,

- sum of 3 triangular numbers,
- sum of 4 square numbers,
- sum of 5 pentagonal numbers,
- sum of 6 hexagonal numbers,
- etc.

History :

- the theorem was stated by Fermat in 1638 without proof,
- square case proved by Lagrange in 1770,
- triangular case proved by Gauß in 1796,
- In general proved by Cauchy in 1813.

Thank you & Happy π-Day !

A bonus challenge : sum of inverse squares

$$\frac{1}{1^2} + \frac{1}{2^2} + \frac{1}{3^2} + \frac{1}{4^2} + \cdots = ?$$