Formalizing a result on polygonal numbers in Lean 4—an experience report

(Joint work with Tomas McNamer)

Kevin Cheung

CanaDAM 2025

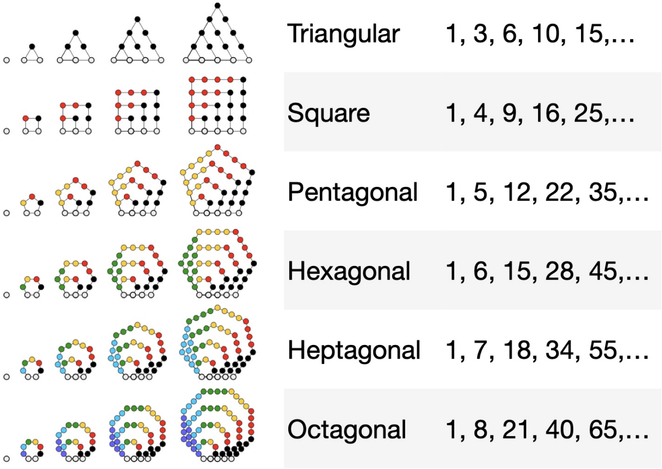
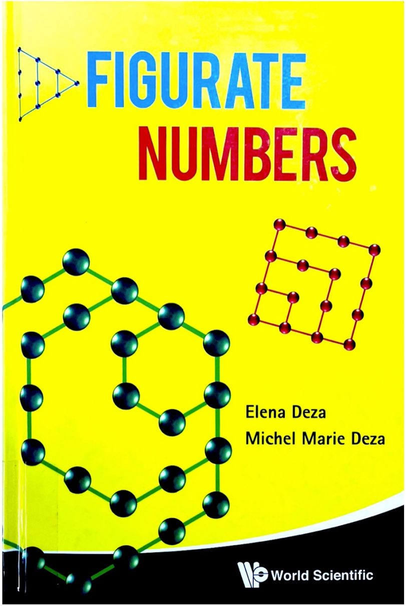


Figure 1: Image by CMC Lee: Licensed under the CC-BY-SA 4.0 license

Figurate numbers



Formulas

- Let s be the number of sides in a polygon where $s \geq 3$.

Formulas

- Let s be the number of sides in a polygon where $s \geq 3$.
- The formula for the kth s-gonal number, where $k \geq 0$, is

$$\frac{(s-2)k^2 - (s-4)k}{2}$$

(By this formula, 0 and 1 are the 0th and 1st s-gonal numbers, resp.)

Formulas

- Let s be the number of sides in a polygon where $s \geq 3$.
- The formula for the kth s-gonal number, where $k \geq 0$, is

$$\frac{(s-2)k^2 - (s-4)k}{2}$$

(By this formula, 0 and 1 are the 0th and 1st s-gonal numbers, resp.)

- For a given s-gonal number $x > 0$, k is given by

$$\frac{\sqrt{8(s-2)x + (s-4)^2} + (s-4)}{2(s-2)}.$$

For example, 10 is the 4th triangular number. The formula gives

$$\frac{\sqrt{8(3-2)10 + (3-4)^2} + (3-4)}{2(3-2)} = 4.$$

Polygonal numbers of order $m + 2$.

- In the literature, it is common to see *polygonal numbers of order* $m + 2$ defined as the integers

$$p_m(k) := \frac{m}{2}\left(k^2 - k\right) + k$$

for $k = 0, 1, 2, \ldots$.

Polygonal numbers of order $m+2$.

- In the literature, it is common to see *polygonal numbers of order* $m+2$ defined as the integers

$$p_m(k) := \frac{m}{2}\left(k^2 - k\right) + k$$

for $k = 0, 1, 2, \ldots$.

- Putting $s = m+2$ in the earlier definition, we have

$$\begin{aligned}\frac{(s-2)k^2 - (s-4)k}{2} &= \frac{mk^2 - (m-2)k}{2} \\ &= \frac{m\left(k^2 - k\right) + 2k}{2} \\ &= \frac{m}{2}\left(k^2 - k\right) + k\end{aligned}$$

Two classical theorems

Theorem (Cauchy). For every integer $m \geq 1$, every nonnegative integer is the sum of $m+2$ polygonal numbers of order $m+2$,

Theorem (Legendre). Let $m \geq 3$.

- If m is odd, then every sufficiently large integer is the sum of four polygonal numbers of order $m+2$.
- If m is even, then every sufficiently large integer is the sum of five polygonal numbers of order $m+2$, one of which is either 0 or 1.

Short proofs by Melvin B. Nathanson (1987)

Nathanson[1] gave a short proof of the following strengthened version of Cauchy's theorem:

Theorem. Let $m \geq 3$ and $n \geq 120m$. Then n is the sum of $m+1$ polygonal numbers of order $m+2$, at most four of which are different from 0 or 1.

A key lemma in the proof also leads to a short proof of Legendre's theorem.

[1] Nathanson, Melvyn B (1987), A short proof of Cauchy's polygonal number theorem, *Proceedings of the American Mathematical Society*, pp. 22–24.

Revised statements and proofs (1996)

However, Nathanson gave the following versions in his book[2]:

Theorem. If $m \geq 4$ and $n \geq 108m$, then n can be written as the sum of $m+1$ polygonal numbers of order $m+2$, at most four of which are different from 0 or 1. If $n \geq 324$, then n can be written as the sum of five pentagonal numbers, at least one of which is 0 or 1.

Theorem. Let $m \geq 3$ and $n \geq 28m^3$. If m is odd, then n is the sum of four polygonal numbers of order $m+2$. If m is even, then n is the sum of five polygonal numbers of order $m+2$, at least one of which is 0 or 1.

Since these versions have been formalized in Isabelle in 2023[3], we decided to formalize in Lean 4 the version of the first theorem that appeared in the 1987 paper.

[2] Nathanson, Melvyn B (1996), *Additive Number Theory*, pp. 27–33.

[3] Kevin Lee, Zhengkun Ye, and Angeliki Koutsoukou-Argyraki (2023), Polygonal Number Theorem, *Archive of Formal Proofs*.

Sum of four pentagonal numbers

Specializing the second theorem to $m = 3$ gives the following:

Theorem. If $n \geq 756$, then n is the sum of four pentagonal numbers.

What is the largest number that cannot be expressed as the sum of four pentagonal numbers?

Ask Question

Asked 2 years, 6 months ago Modified 2 years, 6 months ago Viewed 75 times

1

By Fermat's polygonal number theorem, every number can be written as the sum of five pentagonal numbers. The largest integer I've been able to find that can't be represented as the sum of four pentagonal numbers was 21 (searched up to 21)(I am not good enough at coding to code this up). What is the largest such number?

number-theory

Share Cite Follow

edited Oct 24, 2022 at 15:52

asked Oct 24, 2022 at 15:50
mathlander
4,077 ●2 ■14 ▲43

2 89. See this. Note: I am not confident that this has been proven, just that it has been conjectured and backed up numerically. Similarly, it is conjectured that there are only 210 natural numbers that need more than 3. See this. And this for a general discussion. – lulu Oct 24, 2022 at 15:52

Figure 2: https://math.stackexchange.com/q/4560516

Sequence A133929 at OEIS website

A133929 Positive integers that cannot be expressed using four pentagonal numbers. 2

9, 21, 31, 43, 55, 89

(list; graph; refs; listen; history; text; internal format)

OFFSET 1,1

COMMENTS Equivalently, integers m such that the smallest number of pentagonal numbers (A000326) which sum to m is exactly five, that is, A100878(a(n)) = 5.
Richard Blecksmith & John Selfridge found these six integers among the first million, they believe that they have found them all (Richard K. Guy reference). - Bernard Schott, Jul 22 2022

REFERENCES Richard K. Guy, Unsolved Problems in Number Theory, 3rd Edition, Springer, 2004, Section D3, Figurate numbers, pp. 222-228.

LINKS Table of n, a(n) for n=1..6.
Eric Weisstein's World of Mathematics, Pentagonal Number

EXAMPLE
```
 9 =  5 +  1 + 1 + 1 + 1.
21 =  5 +  5 + 5 + 5 + 1.
31 = 12 + 12 + 5 + 1 + 1.
43 = 35 +  5 + 1 + 1 + 1.
55 = 51 +  1 + 1 + 1 + 1.
89 = 70 + 12 + 5 + 1 + 1.
```

CROSSREFS Cf. A000326, A007527, A100878.
Equals A003679 \ A355660.
Sequence in context: A173460 A110701 A243703 * A325573 A086470 A176256
Adjacent sequences: A133926 A133927 A133928 * A133930 A133931 A133932

Figure 3: https://oeis.org/A133929

The following appears in Richard K. Guy's book[4]:

> *Richard Blecksmith & John Selfridge found six numbers among the first million, namely 9, 21, 31, 43, 55 and 89, which require five pentagonal numbers of positive rank, and two hundred and four others, the largest of which is 33066, which require four. They believe that they have found them all.*

[4] Guy, Richard K. (1996), *Unsolved Problems in Number Theory*, p. 222.

Known but not explicitly stated?

Theorem. Every positive integer $n \notin \{9, 21, 31, 43, 55, 89\}$ can be expressed as the sum of at most four positive pentagonal numbers.

Two strengthenings of Cauchy's theorem

Recall the following:

Theorem (1987 paper). Let $m \geq 3$ and $n \geq 120m$. Then n is the sum of $m+1$ polygonal numbers of order $m+2$, at most four of which are different from 0 or 1.

Theorem (1996 book). If $m \geq 4$ and $n \geq 108m$, then n can be written as the sum of $m+1$ polygonal numbers of order $m+2$, at most four of which are different from 0 or 1. If $n \geq 324$, then n can be written as the sum of five pentagonal numbers, at least one of which is 0 or 1.

Gap in the proof in the paper version

The proof of the theorem in the 1987 paper starts with the following:

> *Let* b_1 *and* b_2 *be consecutive odd integers. The set of numbers of the form* $b + r$*, where* $b \in \{b_1, b_2\}$ *and* $r \in \{0, 1, \ldots, m - 3\}$*, contains a complete set of residue classes modulo* m*.*

- This argument is also in *Figurate Numbers* by Deza & Deza.

Gap in the proof in the paper version

The proof of the theorem in the 1987 paper starts with the following:

> *Let* b_1 *and* b_2 *be consecutive odd integers. The set of numbers of the form* $b + r$*, where* $b \in \{b_1, b_2\}$ *and* $r \in \{0, 1, \ldots, m-3\}$*, contains a complete set of residue classes modulo* m*.*

- This argument is also in *Figurate Numbers* by Deza & Deza.
- The statement fails for $m = 3$. To repair the argument, simply seek three consecutive odd integers instead of two.

Gap in the proof in the paper version

The proof of the theorem in the 1987 paper starts with the following:

> *Let b_1 and b_2 be consecutive odd integers. The set of numbers of the form $b + r$, where $b \in \{b_1, b_2\}$ and $r \in \{0, 1, \ldots, m-3\}$, contains a complete set of residue classes modulo m.*

- This argument is also in *Figurate Numbers* by Deza & Deza.
- The statement fails for $m = 3$. To repair the argument, simply seek three consecutive odd integers instead of two.
- We believe that this gap was known to various individuals (including Nathanson himself). However, in our literature search, we did not come across any mention of this gap.

Reanalysis and improved bounds

We performed a tighter analysis of a key lemma and obtained the following:

Theorem. Let n and m be positive integers. If either

- $m \geq 4$ and $n \geq 53m$; or
- $m = 3$ and $n \geq 159m$,

then n is the sum of $m+1$ polygonal numbers of order $m+2$, at most four of which are different from 0 or 1.

Sum of four pentagonal numbers

Theorem (Nathanson 1996). If $n \geq 756$, then n is the sum of four pentagonal numbers.

Theorem (C. and McNamer 2025). If $n \geq 477$, then n is the sum of four pentagonal numbers.

The cases for $n < 477$ and $n \notin \{9, 21, 31, 43, 55, 89\}$ are verified computationally and can also be checked by hand around an hour.

- Our formalization work in Lean 4 consists of two parts.

Formalization in Lean 4

- Our formalization work in Lean 4 consists of two parts.
- The first is the formalization of

  Theorem (C. and McNamer 2025). If $n \geq 477$, then n is the sum of four pentagonal numbers.

Formalization in Lean 4

- Our formalization work in Lean 4 consists of two parts.
- The first is the formalization of

  Theorem (C. and McNamer 2025). If $n \geq 477$, then n is the sum of four pentagonal numbers.

- The second is defining the decidable instance `IsnPolygonal m n` which facilitates determining if `n` is a polygonal number of order `m` by using the `decide` tactic.

Formalization in Lean 4

- Our formalization work in Lean 4 consists of two parts.
- The first is the formalization of

  Theorem (C. and McNamer 2025). If $n \geq 477$, then n is the sum of four pentagonal numbers.
- The second is defining the decidable instance `IsnPolygonal m n` which facilitates determining if `n` is a polygonal number of order `m` by using the `decide` tactic.
- Around 2700 lines of Lean 4 code in total.

Formalization in Lean 4

- Our formalization work in Lean 4 consists of two parts.
- The first is the formalization of

  Theorem (C. and McNamer 2025). If $n \geq 477$, then n is the sum of four pentagonal numbers.

- The second is defining the decidable instance `IsnPolygonal m n` which facilitates determining if `n` is a polygonal number of order `m` by using the `decide` tactic.
- Around 2700 lines of Lean 4 code in total.
- We discovered the gap when we tried to formalize the proof in the 1987 paper.

Formalization in Lean 4

- Our formalization work in Lean 4 consists of two parts.
- The first is the formalization of

  Theorem (C. and McNamer 2025). If $n \geq 477$, then n is the sum of four pentagonal numbers.
- The second is defining the decidable instance `IsnPolygonal m n` which facilitates determining if `n` is a polygonal number of order `m` by using the `decide` tactic.
- Around 2700 lines of Lean 4 code in total.
- We discovered the gap when we tried to formalize the proof in the 1987 paper.
- The major challenges in the formalization process were dealing with the various types for numbers (`Nat`, `Int`, `Rat`, `Real`) and looking up relevant results in Mathlib.

Future work

- Unlike the formalization in Isabelle, we assumed Gauss' Eureka Theorem[5] without proof since it has not been formalized in Lean 4 as far as we know.

[5] Also known as Gauss' Triangular Number Theorem, it asserts that every positive integer can be represented as the sum of at most three triangular numbers, which is equivalent to that every positive integer congruent to 3 modulo 8 is the sum of three odd squares.

Future work

- Unlike the formalization in Isabelle, we assumed Gauss' Eureka Theorem[5] without proof since it has not been formalized in Lean 4 as far as we know.
- We hope that efforts to formalize Gauss' theorem in Lean 4 will be undertaken in the near future.

[5] Also known as Gauss' Triangular Number Theorem, it asserts that every positive integer can be represented as the sum of at most three triangular numbers, which is equivalent to that every positive integer congruent to 3 modulo 8 is the sum of three odd squares.