Polygonal Number Theorem

Kevin Lee, Zhengkun Ye and Angeliki Koutsoukou-Argyraki

May 14, 2024

Abstract

We formalize the proofs of Cauchy's and Legendre's Polygonal Number Theorems given in Melvyn B. Nathanson's book 'Additive Number Theory: The Classical Bases' [2].

For $m \geq 1$, the k-th polygonal number of order $m+2$ is defined to be $p_m(k) = \frac{mk(k-1)}{2} + k$. The theorems state that:

- 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.
- 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.

We also formalize the proof of Gauss's theorem which states that every non-negative integer is the sum of three triangular numbers.

Contents

Acknowledgements

The project was completed during the 2023 summer internship of the first two authors within the Cambridge Mathematics Placements (CMP) Programme, supervised by the third author and hosted at the Department of Computer Science and Technology, University of Cambridge. All three authors were funded by the ERC Advanced Grant ALEXANDRIA (Project GA 742178) led by Lawrence C. Paulson.

Kevin Lee and Zhengkun Ye wish to thank the Zulip community for help with beginners' questions.

1 Technical Lemmas

We show three lemmas used in the proof of both main theorems.

theory *Polygonal-Number-Theorem-Lemmas*
  imports *Three-Squares.Three-Squares*

begin

1.1 Lemma 1.10 in [2]

This lemma is split into two parts. We modify the proof given in [2] slightly as we require the second result to hold for $l = 2$ in the proof of Legendre's polygonal number theorem.

theorem *interval-length-greater-than-four*:
  fixes $m\ N\ L :: real$
  assumes $m \geq 3$
  assumes $N \geq 2*m$
  assumes $L = (2/3 + sqrt\ (8*N/m - 8)) - (1/2 + sqrt\ (6*N/m - 3))$
  shows $N \geq 108*m \Longrightarrow L > 4$

⟨*proof*⟩

theorem *interval-length-greater-than-lm*:
  fixes $m\ N :: real$
  fixes $L\ l :: real$
  assumes $m \geq 3$
  assumes $N \geq 2*m$
  assumes $L = (2/3 + sqrt\ (8*N/m - 8)) - (1/2 + sqrt\ (6*N/m - 3))$
  shows $l \geq 2 \wedge N \geq 7*l\hat{}2*m\hat{}3 \Longrightarrow L > l*m$

⟨*proof*⟩

lemmas *interval-length-greater-than-2m* [*simp*] = *interval-length-greater-than-lm* [**where** l=*2*, *simplified*]

1.2 Lemma 1.11 in [2]

We show Lemma 1.11 in [2] which is also known as Cauchy's Lemma.

theorem *Cauchy-lemma*:
  fixes $m\ N\ a\ b\ r :: real$
  assumes $m \geq 3\ N \geq 2*m$
  and $0 \leq a\ 0 \leq b\ 0 \leq r\ r < m$
  and $N = m*(a - b)/2 + b + r$
  and $1/2 + sqrt\ (6*N/m - 3) \leq b \wedge b \leq 2/3 + sqrt\ (8*N/m - 8)$
  shows $b\hat{}2 < 4*a \wedge 3*a < b\hat{}2 + 2*b + 4$

⟨*proof*⟩

lemmas *Cauchy-lemma-r-eq-zero* = *Cauchy-lemma* [**where** *r=0*, *simplified*]

1.3 Lemma 1.12 in [2]

lemma *not-one*:
  fixes *a b* :: *nat*
  assumes *a≥1*
  assumes *b≥1*
  assumes ∃ *k1* :: *nat. a* = *2∗k1+1*
  assumes ∃ *k2* :: *nat. b* = *2∗k2+1*
  assumes *b^2* < *4∗a*
  shows *4∗a−b^2* ≠ *1*

⟨*proof*⟩

lemma *not-two*:
  fixes *a b* :: *nat*
  assumes *a≥1*
  assumes *b≥1*
  assumes ∃ *k1* :: *nat. a* = *2∗k1+1*
  assumes *1*:∃ *k2* :: *nat. b* = *2∗k2+1*
  assumes *b^2* < *4∗a*
  shows *4∗a−b^2* ≠ *2*

⟨*proof*⟩

The following lemma shows that given odd positive integers x, y, z and b, where $x \geq y \geq z$, we may pick a suitable integer u where $u = z$ or $u = -z$, such that $b + x + y + u \equiv 0 \pmod 4$.

lemma *suit-z*:
  fixes *b x y z* :: *nat*
  assumes *odd b* ∧ *odd x* ∧ *odd y* ∧ *odd z*
  assumes *x≥y* ∧ *y≥z*
  shows ∃ *u* :: *int.* (*u=z* ∨ *u=−z*) ∧ (*b+x+y+u*) *mod 4* = *0*

⟨*proof*⟩

lemma *four-terms-bin-exp-allsum*:
  fixes *b s t u v* :: *int*
  assumes *b* = *s+t+u+v*
  shows *b^2* = *t^2+u^2+s^2+v^2+2∗t∗u+2* ∗ *s* ∗ *v* + *2∗t* ∗ *s* + *2∗t* ∗ *v* +*2∗u* ∗ *s* +*2∗u* ∗ *v*

⟨*proof*⟩

lemma *four-terms-bin-exp-twodiff*:
  fixes *b s t u v* :: *int*

assumes $b = s+t-u-v$
shows $b\hat{~}2 = t\hat{~}2+u\hat{~}2+s\hat{~}2+v\hat{~}2-2*t*u-2*s*v+2*t*s-2*t*v-2*u*s+2*u*v$

⟨*proof*⟩

If a quadratic with positive leading coefficient is always non-negative, its discriminant is non-positive.

lemma *qua-disc*:
fixes $a\ b\ c$ :: *real*
assumes $a>0$
assumes $\forall x$::*real*. $a*x\hat{~}2+b*x+c \geq 0$
shows $b\hat{~}2 - 4*a*c \leq 0$

⟨*proof*⟩

The following lemma shows for any point on a 3D sphere with radius a, the sum of its coordinates lies between $\sqrt{3a}$ and $-\sqrt{3a}$.

lemma *three-terms-Cauchy-Schwarz*:
fixes $x\ y\ z\ a$ :: *real*
assumes $a > 0$
assumes $x\hat{~}2+y\hat{~}2+z\hat{~}2 = a$
shows $(x+y+z) \geq -sqrt(3*a) \wedge (x+y+z) \leq sqrt(3*a)$

⟨*proof*⟩

We adapt the lemma above through changing the types for the convenience of our proof.

lemma *three-terms-Cauchy-Schwarz-nat-ver*:
fixes $x\ y\ z\ a$ :: *nat*
assumes $a>0$
assumes $x\hat{~}2+y\hat{~}2+z\hat{~}2 = a$
shows $(x+y+z) \geq -sqrt(3*a) \wedge (x+y+z) \leq sqrt(3*a)$

⟨*proof*⟩

This theorem is Lemma 1.12 in [2], which shows for odd positive integers a and b satisfying certain properties, there exist four non-negative integers s, t, u and v such that $a = s^2 + t^2 + u^2 + v^2$ and $b = s + t + u + v$. We use the Three Squares Theorem AFP entry [1].

theorem *four-nonneg-int-sum*:
fixes $a\ b$ :: *nat*
assumes $a \geq 1$
assumes $b \geq 1$
assumes *odd a*
assumes *odd b*
assumes $3:b\hat{~}2 < 4*a$
assumes $3*a < b\hat{~}2+2*b+4$

shows ∃ *s t u v* :: *int*. $s \geq 0 \wedge t \geq 0 \wedge u \geq 0 \wedge v \geq 0 \wedge a = s\hat{}2 + t\hat{}2 + u\hat{}2 + v\hat{}2 \wedge$
$b = s+t+u+v$

⟨*proof*⟩
end

2 Polygonal Number Theorem

2.1 Gauss's Theorem on Triangular Numbers

We show Gauss's theorem which states that every non-negative integer is the sum of three triangles, using the Three Squares Theorem AFP entry [1]. This corresponds to Theorem 1.8 in [2].

theory *Polygonal-Number-Theorem-Gauss*
imports *Polygonal-Number-Theorem-Lemmas*
begin

The following is the formula for the k-th polygonal number of order $m + 2$.

definition *polygonal-number* :: *nat* ⇒ *nat* ⇒ *nat*
where *polygonal-number m k* = $m*k*(k-1)$ *div* 2 + *k*

When $m = 1$, the polygonal numbers have order 3 and the formula represents triangular numbers. Gauss showed that all natural numbers can be written as the sum of three triangular numbers. In other words, the triangular numbers form an additive basis of order 3 of the natural numbers.

theorem *Gauss-Sum-of-Three-Triangles*:
fixes *n* :: *nat*
shows ∃ *x y z*. *n* = *polygonal-number 1 x* + *polygonal-number 1 y* + *polygonal-number 1 z*

⟨*proof*⟩
end

2.2 Cauchy's Polygonal Number Theorem

We will use the definition of the polygonal numbers from the Gauss Theorem theory file which also imports the Three Squares Theorem AFP entry [1].

theory *Polygonal-Number-Theorem-Cauchy*
imports *Polygonal-Number-Theorem-Gauss*
begin

The following lemma shows there are two consecutive odd integers in any four consecutive integers.

lemma *two-consec-odd*:
fixes *a1 a2 a3 a4* :: *int*

assumes *a1−a2 = 1*
assumes *a2−a3 = 1*
assumes *a3−a4 = 1*
shows *∃k1 k2 :: int. {k1, k2} ⊆ {a1, a2, a3, a4} ∧ (k2 = k1+2) ∧ odd k1*

⟨*proof*⟩

This lemma proves that for two consecutive integers b_1 and b_2, and $r \in \{0, 1, \ldots, m-3\}$, numbers of the form $b_1 + r$ and $b_2 + r$ can cover all the congruence classes modulo m.

lemma *cong-classes*:
fixes *b1 b2 :: int*
fixes *m :: nat*
assumes *m ≥ 4*
assumes *odd b1*
assumes *b2 = b1 + 2*
shows *∀N::nat. ∃b::int. ∃r::nat. (r ≤ m−3) ∧ [N=b+r] (mod m) ∧ (b = b1 ∨ b = b2)*

⟨*proof*⟩

The strong form of Cauchy's polygonal number theorem shows for a natural number N satisfying certain conditions, it may 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. This corresponds to Theorem 1.9 in [2].

theorem *Strong-Form-of-Cauchy-Polygonal-Number-Theorem-1*:
fixes *m N :: nat*
assumes *m≥4*
assumes *N≥108∗m*
shows *∃ xs :: nat list. (length xs = m+1) ∧ (sum-list xs = N) ∧ (∀k≤3. ∃a. xs! k = polygonal-number m a)*
∧ (∀ k ∈ {4..m} . xs! k = 0 ∨ xs! k = 1)

⟨*proof*⟩

theorem *Strong-Form-of-Cauchy-Polygonal-Number-Theorem-2*:
fixes *N :: nat*
assumes *N≥324*
shows *∃ p1 p2 p3 p4 r ::nat. N = p1+p2+p3+p4+r ∧ (∃k1. p1 = polygonal-number 3 k1) ∧ (∃k2. p2 = polygonal-number 3 k2)*
∧ (∃k3. p3 = polygonal-number 3 k3) ∧ (∃k4. p4 = polygonal-number 3 k4) ∧ (r = 0 ∨ r = 1)

⟨*proof*⟩
end

2.3 Legendre's Polygonal Number Theorem

We will use the definition of the polygonal numbers from the Gauss Theorem theory file which also imports the Three Squares Theorem AFP entry [1].

theory *Polygonal-Number-Theorem-Legendre*
  imports *Polygonal-Number-Theorem-Gauss*
begin

This lemma shows that under certain conditions, an integer N can be written as the sum of four polygonal numbers.

lemma *sum-of-four-polygonal-numbers*:
  fixes *N m* :: *nat*
  fixes *b* :: *int*
  assumes $m \geq 3$
  assumes $N \geq 2*m$
  assumes $[N = b]$ $(mod\ m)$
  assumes *odd-b*: *odd b*
  assumes $b \in \{1/2 + sqrt\ (6*N/m - 3) .. 2/3 + sqrt\ (8*N/m - 8)\}$
  assumes $N \geq 9$
  shows $\exists k1\ k2\ k3\ k4.\ N = polygonal\text{-}number\ m\ k1 + polygonal\text{-}number\ m\ k2 + polygonal\text{-}number\ m\ k3 + polygonal\text{-}number\ m\ k4$

⟨*proof*⟩

We show Legendre's polygonal number theorem which corresponds to Theorem 1.10 in [2].

theorem *Legendre-Polygonal-Number-Theorem*:
  fixes *m N* :: *nat*
  assumes $m \geq 3$
  assumes $N \geq 28*m\hat{\ }3$
  shows $odd\ m \Longrightarrow \exists k1\ k2\ k3\ k4::nat.\ N = polygonal\text{-}number\ m\ k1 + polygonal\text{-}number\ m\ k2 + polygonal\text{-}number\ m\ k3 + polygonal\text{-}number\ m\ k4$
and $even\ m \Longrightarrow \exists k1\ k2\ k3\ k4\ k5::nat.\ N = polygonal\text{-}number\ m\ k1 + polygonal\text{-}number\ m\ k2 + polygonal\text{-}number\ m\ k3 + polygonal\text{-}number\ m\ k4 + polygonal\text{-}number\ m\ k5 \wedge (k1 = 0 \vee k1 = 1 \vee k2 = 0 \vee k2 = 1 \vee k3 = 0 \vee k3 = 1 \vee k4 = 0 \vee k4 = 1 \vee k5 = 0 \vee k5 = 1)$

⟨*proof*⟩
end

References

[1] A. Danilkin and L. Chevalier. Three squares theorem. *Archive of Formal Proofs*, May 2023. https://isa-afp.org/entries/Three_Squares.html, Formal proof development.

[2] M. B. Nathanson. *Additive Number Theory: The Classical Bases*, volume 164 of *Graduate Texts in Mathematics*. Springer, New York, 1996.