

Polygonal Number Theorem

Kevin Lee, Zhengkun Ye and Angeliki Koutsoukou-Argraki

September 13, 2023

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

1	Technical Lemmas	3
1.1	Lemma 1.10 in [2]	3
1.2	Lemma 1.11 in [2]	3
1.3	Lemma 1.12 in [2]	4
2	Polygonal Number Theorem	6
2.1	Gauss's Theorem on Triangular Numbers	6
2.2	Cauchy's Polygonal Number Theorem	6
2.3	Legendre's Polygonal Number Theorem	8

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  $m\ N\ L :: \text{real}$ 
```

```
  assumes  $m \geq 3$ 
```

```
  assumes  $N \geq 2*m$ 
```

```
  assumes  $L = (2/3 + \text{sqrt}(8*N/m - 8)) - (1/2 + \text{sqrt}(6*N/m - 3))$ 
```

```
  shows  $N \geq 108*m \implies L > 4$ 
```

```
<proof>
```

```
theorem interval-length-greater-than-lm:
```

```
  fixes  $m\ N :: \text{real}$ 
```

```
  fixes  $L\ l :: \text{real}$ 
```

```
  assumes  $m \geq 3$ 
```

```
  assumes  $N \geq 2*m$ 
```

```
  assumes  $L = (2/3 + \text{sqrt}(8*N/m - 8)) - (1/2 + \text{sqrt}(6*N/m - 3))$ 
```

```
  shows  $l \geq 2 \wedge N \geq 7*l^2*m^3 \implies L > l*m$ 
```

```
<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  $m\ N\ a\ b\ r :: \text{real}$ 
```

```
  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  $1/2 + \text{sqrt}(6*N/m - 3) \leq b \wedge b \leq 2/3 + \text{sqrt}(8*N/m - 8)$ 
```

```
  shows  $b^2 < 4*a \wedge 3*a < b^2 + 2*b + 4$ 
```

```
<proof>
```

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

1.3 Lemma 1.12 in [2]

lemma *not-one*:

fixes $a\ b :: \text{nat}$
assumes $a \geq 1$
assumes $b \geq 1$
assumes $\exists k1 :: \text{nat}. a = 2*k1+1$
assumes $\exists k2 :: \text{nat}. b = 2*k2+1$
assumes $b^2 < 4*a$
shows $4*a - b^2 \neq 1$

<proof>

lemma *not-two*:

fixes $a\ b :: \text{nat}$
assumes $a \geq 1$
assumes $b \geq 1$
assumes $\exists k1 :: \text{nat}. a = 2*k1+1$
assumes $1:\exists k2 :: \text{nat}. b = 2*k2+1$
assumes $b^2 < 4*a$
shows $4*a - b^2 \neq 2$

<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 $b\ x\ y\ z :: \text{nat}$
assumes $\text{odd } b \wedge \text{odd } x \wedge \text{odd } y \wedge \text{odd } z$
assumes $x \geq y \wedge y \geq z$
shows $\exists u :: \text{int}. (u=z \vee u=-z) \wedge (b+x+y+u) \bmod 4 = 0$

<proof>

lemma *four-terms-bin-exp-allsum*:

fixes $b\ s\ t\ u\ v :: \text{int}$
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 $b\ s\ t\ u\ v :: \text{int}$

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>

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

lemma *qua-disc:*

fixes $a\ b\ c :: \text{real}$

assumes $a > 0$

assumes $\forall x::\text{real}. a*x^2+b*x+c \geq 0$

shows $b^2 - 4*a*c \leq 0$

<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 $x\ y\ z\ a :: \text{real}$

assumes $a > 0$

assumes $x^2+y^2+z^2 = a$

shows $(x+y+z) \geq -\text{sqrt}(3*a) \wedge (x+y+z) \leq \text{sqrt}(3*a)$

<proof>

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

lemma *three-terms-Cauchy-Schwarz-nat-ver:*

fixes $x\ y\ z\ a :: \text{nat}$

assumes $a > 0$

assumes $x^2+y^2+z^2 = a$

shows $(x+y+z) \geq -\text{sqrt}(3*a) \wedge (x+y+z) \leq \text{sqrt}(3*a)$

<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 $a\ b :: \text{nat}$

assumes $a \geq 1$

assumes $b \geq 1$

assumes *odd* a

assumes *odd* b

assumes $3*b^2 < 4*a$

assumes $3*a < b^2+2*b+4$

```

shows  $\exists s t u v :: \text{int. } s \geq 0 \wedge t \geq 0 \wedge u \geq 0 \wedge v \geq 0 \wedge a = s^2 + t^2 + u^2$ 
 $+ v^2 \wedge$ 
 $b = s+t+u+v$ 

```

```

⟨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  $\Rightarrow$  nat  $\Rightarrow$  nat
where polygonal-number  $m k = m*k*(k-1) \text{ div } 2 + k$ 

```

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  $n :: \text{nat}$ 
shows  $\exists x y z. n = \text{polygonal-number } 1 x + \text{polygonal-number } 1 y + \text{polygonal-number } 1 z$ 

```

```

⟨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  $a1 a2 a3 a4 :: \text{int}$ 

```

assumes $a1 - a2 = 1$
assumes $a2 - a3 = 1$
assumes $a3 - a4 = 1$
shows $\exists k1\ k2 :: int. \{k1, k2\} \subseteq \{a1, a2, a3, a4\} \wedge (k2 = k1 + 2) \wedge odd\ k1$

<proof>

This lemma proves that for two consecutive integers b_1 and b_2 , and $r \in \{0, 1, \dots, m - 3\}$, 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 $m \geq 4$
assumes $odd\ b1$
assumes $b2 = b1 + 2$
shows $\forall N :: nat. \exists b :: int. \exists r :: nat. (r \leq m - 3) \wedge [N = b + r] (mod\ m) \wedge (b = b1 \vee b = b2)$

<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 $m \geq 4$
assumes $N \geq 108 * m$
shows $\exists xs :: nat\ list. (length\ xs = m + 1) \wedge (sum\ list\ xs = N) \wedge (\forall k \leq 3. \exists a. xs!k = polygonal\ number\ m\ a) \wedge (\forall k \in \{4..m\}. xs!k = 0 \vee xs!k = 1)$

<proof>

theorem *Strong-Form-of-Cauchy-Polygonal-Number-Theorem-2*:

fixes $N :: nat$
assumes $N \geq 324$
shows $\exists p1\ p2\ p3\ p4\ r :: nat. N = p1 + p2 + p3 + p4 + r \wedge (\exists k1. p1 = polygonal\ number\ 3\ k1) \wedge (\exists k2. p2 = polygonal\ number\ 3\ k2) \wedge (\exists k3. p3 = polygonal\ number\ 3\ k3) \wedge (\exists k4. p4 = polygonal\ number\ 3\ k4) \wedge (r = 0 \vee r = 1)$

<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  $\exists k1\ k2\ k3\ k4. N = polygonal-number\ m\ k1 + polygonal-number\ m\ k2 +$ 
   $polygonal-number\ m\ k3 + polygonal-number\ m\ k4$ 
```

<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  $N \geq 28*m^3$ 
  shows odd  $m \implies \exists k1\ k2\ k3\ k4::nat. N = polygonal-number\ m\ k1 + polygonal-number\ m\ k2 +$ 
   $polygonal-number\ m\ k3 + polygonal-number\ m\ k4$ 
  and even  $m \implies \exists k1\ k2\ k3\ k4\ k5::nat. N = polygonal-number\ m\ k1 + polygonal-number\ m\ k2 +$ 
   $polygonal-number\ m\ k3 + polygonal-number\ m\ k4 + polygonal-number\ m\ k5 \wedge (k1 = 0 \vee k1 = 1 \vee k2 = 0 \vee k2 = 1 \vee k3 = 0 \vee k3 = 1 \vee k4 = 0 \vee k4 = 1 \vee k5 = 0 \vee k5 = 1)$ 
```

<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.