Cauchy's Polygonal Numbers

Tomas McNamer

June 17, 2025

Definition 1 (Polygonal Number)**.** An integer n is said to be polygonal of order m if:

$$\exists k \in \mathbb{Z} \quad n = \frac{m-2}{2} \cdot (k \cdot (k-1)) + k$$

Definition 2 (I ub)**.**

$$I_{ub} : \mathbb{Z} \times \mathbb{Z} \to \mathbb{R}$$
$$I_{ub} : (n, m) \mapsto 2 \cdot \left(1 - \frac{2}{m}\right) + \sqrt{4 \cdot \left(1 - \frac{2}{m}\right)^2 + 8 \cdot \left(\frac{n - (m-3)}{m}\right)}$$

Where I_{ub} is non-computable in Lean.

Definition 3 (I lb)**.**

$$I_{ub} : \mathbb{Z} \times \mathbb{Z} \to \mathbb{R}$$
$$I_{ub} : (n, m) \mapsto 2 \cdot \left(1 - \frac{2}{m}\right) + \sqrt{4 \cdot \left(1 - \frac{2}{m}\right)^2 + 8 \cdot \left(\frac{n - (m-3)}{m}\right)}$$

Where I_{lb} is non-computable in Lean.

Lemma 4 (Interval)**.** *Let $n, m \in \mathbb{Z}$ with $m \geq 3$.*

$$m \geq 4 \land n \geq 53 \cdot m \implies I_{ub}(n, m) - I_{lb}(n, m) > 4.002$$

Further,

$$m = 3 \land n \geq 159 \cdot m \implies I_{ub}(n, m) - I_{lb}(n, m) > 6.002$$

That is, the length of the interval $I_{ub}(n, m) - I_{lb}(n, m)$ is greater than 4.002 or 6.002, when $m \geq 4$ or $m = 3$ respectively.

Proof. With $m \geq 4$, we have

$$\begin{aligned} u(n,m) - \ell(n,m) &= \frac{3}{2} - \frac{1}{m} + \sqrt{8\left(\frac{n}{m}\right) + \frac{16}{m^2} + \frac{8}{m} - 4} - \sqrt{6\left(\frac{n}{m}\right) - \frac{3}{m}\left(1 - \frac{3}{m}\right) - \frac{15}{4}} - 0.002 \\ &\geq \frac{3}{2} - \frac{1}{4} + \sqrt{8\left(\frac{n}{m}\right) - 4} - \sqrt{6\left(\frac{n}{m}\right) - \frac{15}{4}} - 0.002 \\ &= \frac{5}{4} + \sqrt{8\left(\frac{n}{m}\right) - 4} - \sqrt{6\left(\frac{n}{m}\right) - \frac{15}{4}} - 0.002 \\ &\geq 4 \end{aligned}$$

by Corollary 3.5 with $x = \frac{n}{m}$. When $m = 3$, we have

$$\begin{aligned} u(n,m) - \ell(n,m) &= \frac{7}{6} + \sqrt{8\left(\frac{n}{m}\right) + \frac{4}{9}} - \sqrt{6\left(\frac{n}{m}\right) - \frac{15}{4}} - 0.002 \\ &\geq 6 \end{aligned}$$

by Corollary 3.6 with $x = \frac{n}{m}$. □

Lemma 5 (qub)**.** *Let $p \in \mathbb{R}$, $c > 0$, $x \leq 0$, and $x < \frac{p}{2} + \sqrt{\left(\frac{p}{2}\right)^2 + c}$, then:*

$$x^2 - p \cdot x - c < 0$$

Proof. Since $c > 0$, we have $\pm\frac{p}{2} + \sqrt{\left(\frac{p}{2}\right)^2 + c} > \pm\frac{p}{2} + \left|\frac{p}{2}\right| \geq 0$. The statement holds trivially when $x = 0$. Assume that $x > 0$. Since $x < \frac{p}{2} + \sqrt{\left(\frac{p}{2}\right)^2 + c}$, we have $x - p < -\frac{p}{2} + \sqrt{\left(\frac{p}{2}\right)^2 + c}$. Thus,

$$\begin{aligned}
x^2 - px - c &= x(x-p) - c \\
&< x\left(-\frac{p}{2} + \sqrt{\left(\frac{p}{2}\right)^2 + c)}\right) - c \\
&< \left(\frac{p}{2} + \sqrt{\left(\frac{p}{2}\right)^2 + c}\right)\left(-\frac{p}{2} + \sqrt{\left(\frac{p}{2}\right)^2 + c)}\right) - c \\
&= 0.
\end{aligned}$$

□

Lemma 6 (qlb)**.** *Let $p \in \mathbb{R}$, $c > 0$, and $x > \frac{p}{2} + \sqrt{\left(\frac{p}{2}\right)^2 + c}$, then:*

$$x^2 - p \cdot x - c > 0$$

Proof. Since $x > \frac{p}{2} + \sqrt{\left(\frac{p}{2}\right)^2 + c} > 0$, we have $x - p > -\frac{p}{2} + \sqrt{\left(\frac{p}{2}\right)^2 + c} > -\frac{p}{2} + \sqrt{\left(\frac{p}{2}\right)^2 + c} > 0$. Hence,

$$\begin{aligned}
x^2 - px - c &= x(x-p) - c \\
&> \left(\frac{p}{2} + \sqrt{\left(\frac{p}{2}\right)^2 + c}\right)(x-p) - c \\
&> \left(\frac{p}{2} + \sqrt{\left(\frac{p}{2}\right)^2 + c}\right)\left(-\frac{p}{2} + \sqrt{\left(\frac{p}{2}\right)^2 + c)}\right) - c \\
&= 0.
\end{aligned}$$

□

Lemma 7 (I lb pos)**.** *Let $n, m, b, r \in \mathbb{Z}$ with $0 \leq r \leq m - 3$, $b > I_{lb}(n,m)$, $3 \leq m$, $2 \cdot m \leq n$ then:*

$$b > 0$$

i.e., $I_{lb}(n,m) > 0$ with the above assumptions.

Proof. Note that

$$\begin{aligned}
b \geq \ell(n,m) &= \left(\frac{1}{2} - \frac{3}{m}\right) + \sqrt{\left(\frac{1}{2} - \frac{3}{m}\right)^2 + 6\left(\frac{n}{m}\right) - 4} + 0.001 \\
&> \left(1 - \frac{6}{m}\right)/2 + \sqrt{\left(\left(1 - \frac{6}{m}\right)/2\right)^2 + 6\left(\frac{n-r}{m}\right) - 4}
\end{aligned}$$

Setting $p := 1 - \frac{6}{m}$ and $c := 6\left(\frac{n-r}{m}\right) - 4$, we have $c > 0$ and so, by Lemma 6 part (b), we obtain that $b^2 + 2b + 4 - 3a = b^2 - \left(1 - \frac{6}{m}\right)b - \left(6\left(\frac{n-r}{m}\right) - 4\right) > 0$. □

Lemma 8 (main)**.** *Let $n, m, b, r \in \mathbb{Z}$ where b is odd, with $0 \le r \le m-3$, $2 \cdot m \le n$, $I_{lb}(n,m) \le b \le I_{ub}(n,m)$, and $m \mid (n-b-r)$ then:*

$$a = 2 \cdot \frac{n-b-r}{m} + b$$

and,

$$a \text{ is odd and } b^2 - 4 \cdot a < 0 \text{ and } b^2 + 2 \cdot b + 4 - 3 \cdot a > 0$$

Proof. Note that

$$\begin{aligned} b \ge \ell(n,m) &= \left(\frac{1}{2} - \frac{3}{m}\right) + \sqrt{\left(\frac{1}{2} - \frac{3}{m}\right)^2 + 6\left(\frac{n}{m}\right) - 4} + 0.001 \\ &> \left(1 - \frac{6}{m}\right)/2 + \sqrt{\left(\left(1 - \frac{6}{m}\right)/2\right)^2 + 6\left(\frac{n-r}{m}\right) - 4} \end{aligned}$$

Setting $p := 1 - \frac{6}{m}$ and $c := 6\left(\frac{n-r}{m}\right) - 4$, we have $c > 0$ and so, by Lemma 6 part (b), we obtain that $b^2 + 2b + 4 - 3a = b^2 - \left(1 - \frac{6}{m}\right) b - \left(6\left(\frac{n-r}{m}\right) - 4\right) > 0$. We can also see from the above derivation that $b > 0$. Now,

$$\begin{aligned} b \le u(n,m) &= 2\left(1 - \frac{2}{m}\right) + \sqrt{4\left(1 - \frac{2}{m}\right)^2 + 8\left(\frac{n-(m-3)}{m}\right)} - 0.001 \\ &< \left(4\left(1 - \frac{2}{m}\right)/2\right) + \sqrt{\left(4\left(1 - \frac{2}{m}\right)/2\right)^2 + 8\left(\frac{n-r}{m}\right)}. \end{aligned}$$

Setting $p := 4\left(1 - \frac{2}{m}\right)$ and $c := 8\left(\frac{n-r}{m}\right)$, we have $c > 0$ (as $n - r \ge 2m - (m-3) = m + 3$) and so, by Lemma 5 part (a), we obtain that $b^2 - 4a = b^2 - 4\left(1 - \frac{2}{m}\right) b - \frac{8n-r}{m} < 0$.

□

Theorem 9 (mod m congr)**.** *Let b_1, b_2 be integers such that $b_2 = b_1 + 2$, and let $n \in \mathbb{Z}$, and $m \in \mathbb{N}$ such that $m \ge 4$. Then:*

$$\exists\ r \in \mathbb{Z} \text{ such that } 0 \le r \le m-3 \text{ and } \exists\ b \in \{b_1, b_2\} \text{ such that } n \equiv b + r \pmod{m}$$

Lemma 10 (blist)**.** *Let $p, q \in \mathbb{R}$, $k \in \mathbb{N}$ such that $q - p \ge 2 \cdot k$, then:*

There exists a sequence $(b_i)_0^{k-1}$ of k integers, and an integer m such that:

$$\forall\ (i = 0, \dots, k-1), b_i = 2 \cdot (m+i) + 1 \wedge p \le b_i \le q$$

Proof. Let $\ell = \lceil p \rceil$.

Note that $p > \ell - 1$.

We can take m to be the least integer such that $2m + 1 \ge \ell$. Indeed, for all $i = 0, \dots, k-1$, we have that $b_i \ge b_0 = 2m + 1 \ge p$ and $b_i \le b_{k-1} = 2(m + (k-1)) + 1 = 2m + 1 + 2(k-1)$.

If ℓ is even, then $2m + 1 = \ell + 1$.

Hence,

$$\begin{aligned}2m+1+2(k-1) &= \ell+1+2(k-1)\\ &= \ell-1+2k\\ &< p+2k\\ &\le p+q-p\\ &= q\end{aligned}$$

If ℓ is odd, then $2m+1=\ell$.
Hence,

$$\begin{aligned}2m+1+2(k-1) &= \ell+2(k-1)\\ &= \ell-1+2k-1\\ &< p+2k+1\\ &\le p+q-p-1\\ &< q\end{aligned}$$

□

Lemma 11 (res b)**.** *Let $n \in \mathbb{Z}$, and $b_1, b_2, b_3 \in \mathbb{Z}$ such that $b_2 = b_1 + 2$ and $b_3 = b_2 + 2$. Then there exists $b \in \{b_1, b_2, b_3\}$ such that:*

$$3 \mid n - b$$

Proof. Proof by cases on $n \mod b_1$ □

Lemma 12 (res b r)**.** *Let $b_1, b_2 \in \mathbb{Z}$, $b_2 = b_1 + 2$, and $n, m \in \mathbb{Z}$ such that $m \ge 4$, then:*

$$\exists\, r \in \mathbb{Z} \text{ such that } 0 \le r \le m-3 \text{ and } (m \mid (n - b_1 - r)) \vee (m \mid (n - b_2 - r))$$

Proof. Proof by cases on $n \mod b_1$ □

Lemma 13 (b r)**.** *Let n, m be positive integers such that $m \ge 4$ and $n \ge 53 \cdot m$ or if $m = 3$, $n \ge 159 \cdot m$. Then there exists integers b, r such that:*

1. *b is odd*
2. *$I_{lb}(n,m) \le b \le I_{ub}(n,m)$*
3. *$0 \le r \le m-3$*
4. *$m \mid (n - b - r)$*

Proof. First, consider the case when $m \ge 4$ and $n \ge 53m$. By Lemma 4 part (a), we have $u(n,m) - \ell(n,m) \ge 4$. It follows from Lemma 10 that there exist odd integers b_0, b_1 in the interval $[\ell(n,m), u(n,m)]$ such that $b_1 = b_0 + 2$. Let r' be the remainder when $n - b_0$ is divided by m. Note that $r' \le m-1$ and $n - b_0 - r' \equiv 0 \pmod m$. If $r' \ge m-2$, set r to $r'-2$ and b to b_1. Since $r' \le m-1$, we have that $r = r'-2 \le m-3$. Also, $r = r'-2 \ge m-2-2 = m-4 \ge 4-4 = 0$. Then setting b to b_1, we have that $n - b - r = n - b_1 - (r'-2) = n - b_0 - r' \equiv 0 \pmod m$. Hence, m divides $n-b-r$. Otherwise, we have $r' \le m-3$. Setting r to r' and b to b_0, we have that $n - b - r = n - b_0 - r' \equiv 0 \pmod m$. Hence, m divides $n-b-r$. Next, consider the case when $m = 3$ and $n \geq 159m$. We set r to 0. By Lemma 4 part (b), we have $u(n,m) - \ell(n,m) \geq 6$. It follows from Lemma 10 that there exist odd integers b_0, b_1, b_2 in the interval $[\ell(n,m), u(n,m)]$ such that $b_1 = b_0 + 2$ and $b_2 = b_1 + 2$. Since $b_1 \equiv b_0 + 2 \pmod 3$ and $b_2 \equiv b_1 + 2 \equiv b_0 + 4 \equiv b_0 + 1 \pmod 3$, it follows that for some $b \in \{b_0, b_1, b_2\}$, we have $n - b - r \equiv n - b \equiv 0 \pmod 3$. ☐

Lemma 14 (Cauchy's Lemma). *Let a, b be odd positive integers such that $b^2 < 4a$ and $3a < b^2 + 2b + 4$, then there exists nonnegative integers s, t, u, v such that:*

$$a = s^2 + t^2 + u^2 + v^2 \quad \textit{and} \quad b = s + t + u + v$$

Proof. Omitted. ☐

Theorem 15 (Cauchy's Polygonal Number Theorem).

Let $m, n \in \mathbb{N}$ such that $m \geq 3$, and $n \geq 120 \cdot m$ and if $m \geq 4$, $n \geq 53 \cdot m$ or if $m = 3$, $n \geq 159 \cdot m$.

Then S is the sum of $m + 1$ polygonal numbers of order $m + 2$.