

# An Algebraic Study on Star Patterns.

Rohan Thomas

August 25, 2024

## 1 Introduction

Consider the problem of drawing star patterns. If you are asked to draw a 5 pointed star pattern, it is relatively straight forward. How about an 8 pointed star pattern?. It could be challenging at first. To do this, start by drawing a circle and then mark equally spaced 8 points and label them 0, 1, 2, 3,  $\dots$ , 7. Next, connect each point to another point which is at a fixed units away. For instance, let us decide to connect every point to points which are 3 units away. This means we can connect 0 to 3, 3 to 6,  $\dots$ , 5 to 0 to obtain Fig 1.1.

On the other hand, if the choice is to connect every point to points that are 2 units away, this choice forms a star pattern having two distinct components. To draw this pattern, we can connect 0 to 2, 2 to 4,  $\dots$ , 6 to 0 for the first component, and then connect 1 to 3, 3 to 5,  $\dots$ , 7 to 1 to obtain Fig 1.2. Notice that the choice of turning by 3 results in construction without lifting pen; such a pattern is called as a *star polygon*. In contrast, when connecting 2 units away requires lifting the pen, and this pattern is referred to as a *star figure*. This means, star patterns are generally classified into star polygons and star figures.

These patterns are commonly denoted using Schläfli symbol  $\{n/k\}$ , where  $n$  is the number of vertices and  $k$  is turning number. The star polygon obtained from connecting every third is denoted as  $\{8/3\}$ , while the star figure drawn by connecting every two units apart is denoted as  $\{8/2\}$ .

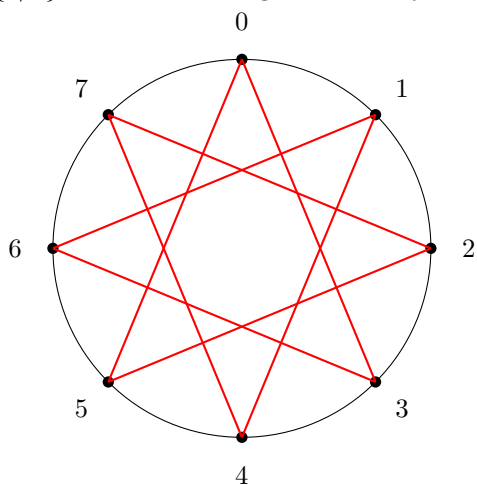


Fig 1.1 Star Polygon  $\{8/3\}$

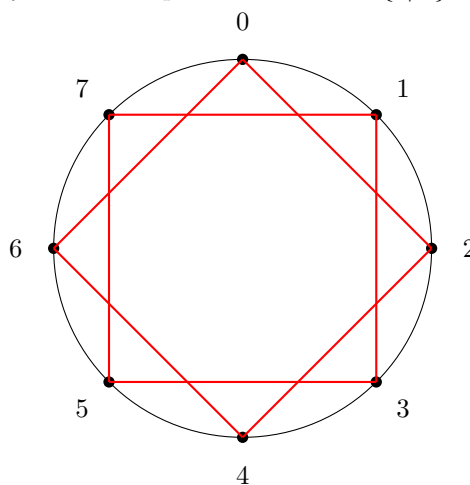


Fig 1.2 Star Figure  $\{8/2\}$

It's a fun activity to observe and make conjectures about these patterns. For instance, How many  $n$  pointed star polygons can be drawn, or How many distinct components are there in a star figure. We will discuss the algebraic connections in star polygons and figures to answer these questions. In fact, these patterns will help us to visualize abstract concepts from Group theory such as cyclic

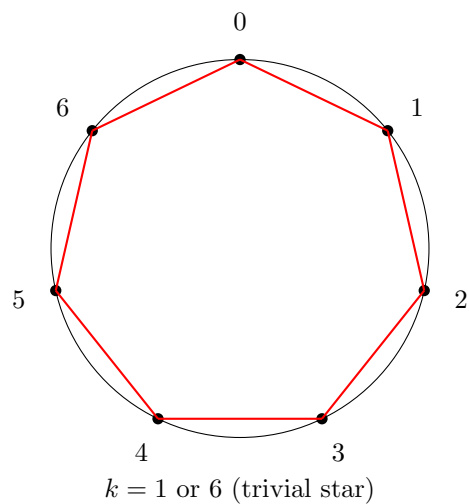
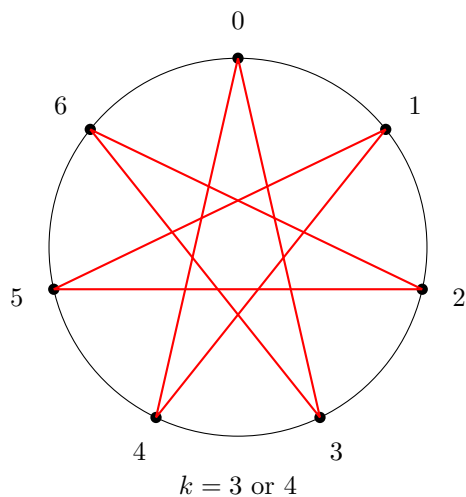
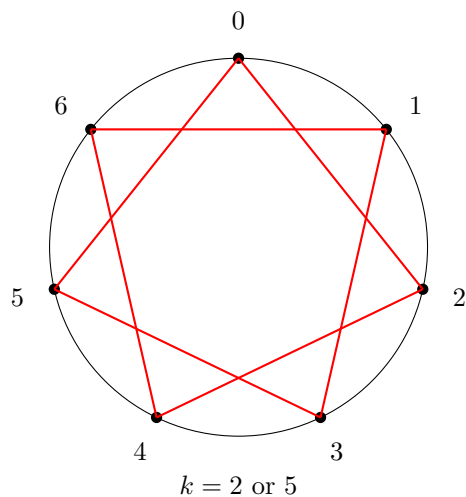
groups, isomorphism and cosets. Let us begin by considering the construction and discussion of star patterns without lifting the pen or better known as star polygons.

## 2 Star Polygons: Construction and Their Cyclic Structure

As suggested in the introduction, when constructing a star polygon, we need to choose the turning number such that it doesn't loop in a smaller subset of the labels but reach all them. This is exactly the situation when we choose  $k$  such that  $\gcd(k, n) = 1$

Draw a circle and mark  $n$  points and label them with numbers from 0 to  $n - 1$ . Choose any number  $k$  such that  $\gcd(k, n) = 1$ . Join each point  $x$  to  $(x + k) \pmod{n}$ .

For instance, The following are possible 7 pointed star polygons based on this procedure:



In this section, we will mainly address following questions:

- Why the condition  $\gcd(k, n) = 1$ ?
- How many  $n$  pointed star polygons can be drawn. ?
- Why do star polygon symmetries pair up ?

In addition to answer these questions, we need to understand cyclic groups, the underlying algebra structure associated with these patterns. In fact they help to visualize cyclic groups. Let us first introduce the notion of a cyclic group.

## Cyclic Groups; An overview

Given a set  $G$  together with an binary operation  $*$ , we say  $G$  forms an algebraic structure named *group*, if it satisfies the following axioms,

1.  $*$  is a binary operation in  $G$
2.  $a * (b * c) = (a * b) * c, \forall a, b, c \in G$
3. there exist  $e \in G$  such that  $a * e = e * a = a$
4. for each  $a \in G$  there exist  $b$  such that  $a * b = e = b * a$

A group  $G$  is said to be *cyclic*, if there exist  $a \in G$  such that  $G = \{a^n : n \in \mathbb{Z}\}$ , where ' $a$ ' is called as the generator. In other words, a cyclic group posses an element that can generate all other elements in the group. An important example of cyclic group is an additive group. Let  $\mathbb{Z}_n = \{0, 1, 2, 3, \dots, (n-1)\}$  be the set of remainders upon division by  $n$ , we can easily verify  $\mathbb{Z}_n$  is a group under addition modulo  $n$ . Since  $1 \in \mathbb{Z}_n$ , clearly it is cyclic.

The construction procedure suggested earlier be thought as constructing over the cyclic group  $\mathbb{Z}_n$ . We can think of wrapping around elements of  $\mathbb{Z}_n$  around the circle, , choosing an element  $k$  from  $\mathbb{Z}_n$  and connecting the points by computing  $k, (k +_n k), (k +_n k +_n k), \dots, 0$ .

## Why the condition $\gcd(k, n) = 1$ ?

As our intuition suggests, an  $n$  pointed star polygons is only possible when the choice of  $k$  is a generator of the group  $\mathbb{Z}_n$ . If you observe Fig 2.1, we can note that when  $m = 8$  and  $k = 2$ , this choice reaches all the multiples of 2. Similarly,  $k = 6$  reaches the same labels. What's common between them ? They share the greatest common divisor of 2 with  $m = 8$ . In fact, when we choose some  $k$ , the labels it will reach are multiples  $\gcd(k, n)$ . So naturally to reach all the labels  $\gcd(k, n)$  simply has to be 1. The following theorem proves it formally using bezout's identity and congruence properties.

**Theorem 2.1**  $k \in \mathbb{Z}_n$  is a generator of  $\mathbb{Z}_n$ , if  $\gcd(k, n) = 1$

**Proof:** The idea of proof is similar to earlier discussion. We have to show that, if  $\gcd(k, n) = 1$ , then the successive elements  $k, (k +_n k), (k +_n k +_n k)$ , somehow reaches 1. If it can reach 1 then it must reach any arbitrary  $b \in \mathbb{Z}_n$ .

Applying bezout's identity in  $\gcd(a, n) = 1$ , we get  $x_0, y_0$  such that  $ax_0 + ny_0 = 1$ . Rearranging we get,  $ax_0 - 1 = n(-y_0)$ . From the definition of congruence, this will imply  $ax_0 \equiv 1 \pmod{n}$ . Now let  $b \in \mathbb{Z}_n$  be arbitrary , using the multiplication property of congruence we get

$$a(x_0 b) \equiv (b) \pmod{n} \implies \underbrace{a +_n a +_n \dots +_n a}_{x_0 b \text{ times}} = b$$

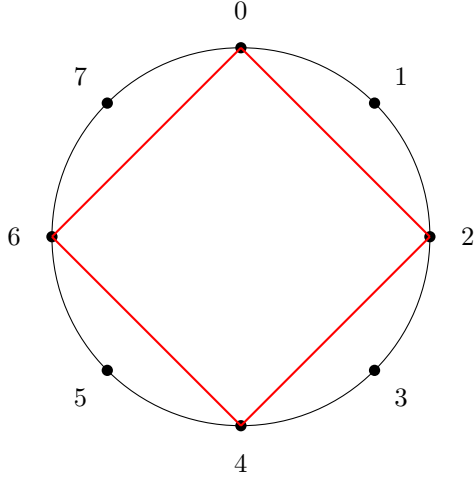


Fig 2.1 ( $k = 2$  or  $6$ )

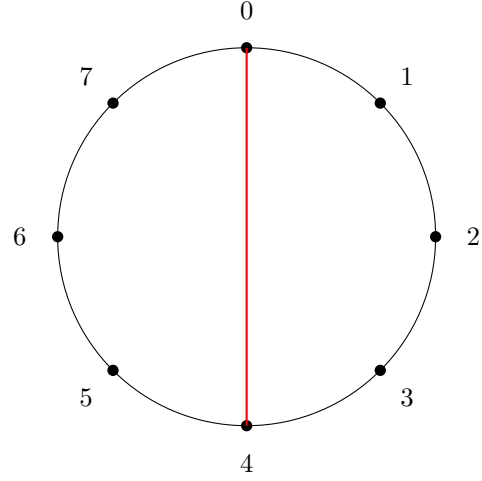


Fig 2.2 ( $k = 4$ )

Though the choice of  $k = 2$  and  $k = 4$  didn't draw the star but they help to visualize subgroups of  $\mathbb{Z}_8$ . Fig 2.1 represents the cyclic subgroup generated by 2 or  $\langle 2 \rangle = \{0, 2, 4, 6\}$  and Fig 2.2 represents  $\langle 4 \rangle = \{4, 0\}$ .

### How many $n$ pointed star polygons can be drawn ?

We expect to draw a star polygon for each  $k \in \mathbb{Z}_n$  such that  $\gcd(k, n) = 1$ . Therefore, counting those elements less than  $n$  and relatively prime to  $n$  will give us the possible choices of  $k$ . This is exactly same situation with Euler's Totient Function  $\phi(n)$ . Intuitively, we can see that each clockwise-construction is paired off with a counter-clockwise construction. Therefore, there are  $\frac{\phi(n)}{2}$  distinct star polygons (counting the trivial star polygon). For instance, when  $m = 8$ ,  $\phi(8) = 4$ , so the two distinct star patterns; The trivial star and Fig 1.1

### Why do symmetries pair up?

The fact that counter clock-wise constructions with  $k$  is always paired off with clockwise construction with  $(n - k)$  can be seen as a geometrical argument for why Euler's Totient Function is always even. Formally, if  $k \in \mathbb{Z}_n$  is a generator then  $(n - k)$  is also a generator of  $\mathbb{Z}_n$ .

**Theorem 2.2** if  $\gcd(k, n) = 1$  then  $\gcd(n - k, n) = 1$

**Proof** (By contra-position): Suppose  $\gcd(m - k, m) = d \neq 1$ . Thus  $d|(m - k)$  and  $d|m$ . from  $d|(m - k)$  we get  $(m - k) = dk$ , for some  $k \in \mathbb{Z}$ . also from  $d|m$  we get  $m = dl$ , for some  $l \in \mathbb{Z}$

We can easily replace  $m$  and see,  $dl - k = dk \implies k = d(l - k)$ . Thus  $d|k$ , but notice since  $d > 1$  this contradicts  $(k, m) = 1$  being greatest common divisor. Hence  $(m - k, m) = 1$

The proof effectively tells us that  $k$  and  $(n - k)$  as not just additive inverse in the additive group but they both generator of the group.

Finally, We are looking for the smallest possible non trivial star. Since the generators are always paired up. We need  $\phi(n) = 4$ , so that two choices belongs to trivial star and other two are our desired. This happens when we have  $n = 5$ , because  $\phi(5) = 4$  Therefore, the smallest possible star is our familiar 5 pointed star.

### 3 Multiplicative Construction

In the previous section, we considered the successive elements in additive fashion to construct the pattern. How about trying to draw star polygons in a multiplicative fashion ?. This means, choose some label and repeatedly multiply it to reach all elements of the set. Clearly, we have to modify set of labels, since repeated multiplication goes to 1 instead of 0.

We can start the labels  $\{1, 2, 3, \dots, n\}$ , and ask which choice of  $k$ , under repeated multiplication reaches all elements of this set. More formally, we are in fact looking at the set that forms a group under multiplication modulo  $n$ , denoted as  $U(n) = \{x : \gcd(x, n) = 1\}$ , and asking, when is this group cyclic or posses some element upon repeated multiplication it can help to reach all others.

If you are familiar with cryptography, figuring out when  $U(n)$  is cyclic better known as the **Discrete Logarithm Problem**.

] This preparation of this material is on going. Last Updated: August 25, 2024