MIT PRIMES Circle

Number Theory: Why *MIT PRIMES Circle* Could be Renamed *MIT PRIMES Triangle*

By Boston Bulis, Kyra Burke, and Lee Van Voorhis

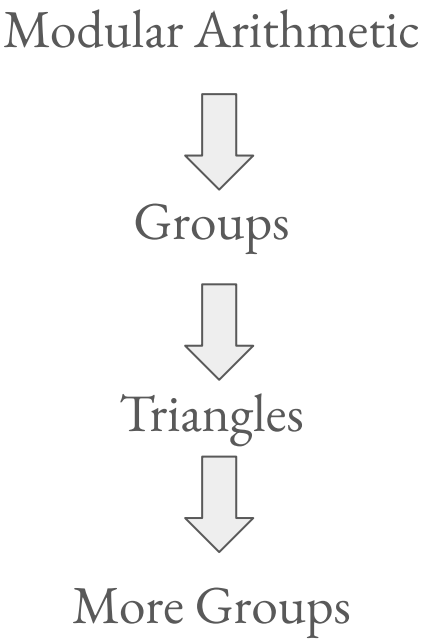
Mentor Sam Packman

May 18th, 2025

PRIMES

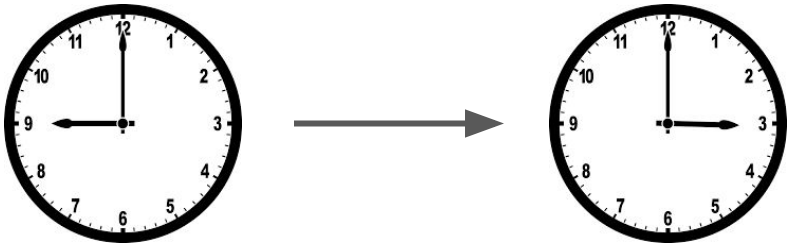
Groups? Triangles? Modular Arithmetic?

A friendly roadmap!



What is Modular Arithmetic?

$$15 \equiv 3 (\text{mod } 12)$$



$$b \equiv r (\text{mod } m)$$

Two integers (b and r) being equivalent, or congruent, (mod m) means that the difference between b and r is divisible by m. In other words, there exists some integer x for which $b - r = mx$.

Properties of Modular Arithmetic

If $a \equiv c \pmod{m}$ and $b \equiv d \pmod{m}$, then:

- Addition

$$a + b \equiv c + d \pmod{m} \quad 15 + 12 \equiv 5 + 2 \pmod{10}$$

- Multiplication

$$a \times b \equiv c \times d \pmod{m} \quad 7 \times 11 \equiv 1 \times 2 \pmod{3}$$

What is a Group?

A **group** is a set of elements (elt) with an operation (ex: $\oplus$) that satisfies four axioms:

1. **Closure:** Combining any two elements using $\oplus$ gives another element in the set

2. **Associativity:** $(a \oplus b) \oplus c = a \oplus (b \oplus c)$ for any elts. a, b and c

3. **Identity:** There's an element e such that $a \oplus e = a$ for any elt. a

4. **Inverses:** Every element a has an inverse (often denoted a^{-1}) for which $a \oplus a^{-1} = e$.

The Integer Group

$(\mathbb{Z}, +)$ Set of integers closed under addition

1. **Closure:** Adding to integers $\rightarrow$ another integer
2. **Associativity:** $(a + b) + c = a + (b + c)$ always works with any integers a, b, and c
3. **Identity:** 0 is an integer, and $a + 0 = a$ for any integer a
4. **Inverses:** For every integer a, it has an inverse $-a \rightarrow a + (-a) = 0$

Modular Arithmetic and Groups

$$\mathbb{Z}_6^+ = \{0, 1, 2, 3, 4, 5\}$$

Operation: addition modulo 6

+	0	1	2	3	4	5
0	0	1	2	3	4	5
1	1	2	3	4	5	0
2	2	3	4	5	0	1
3	3	4	5	0	1	2
4	4	5	0	1	2	3
5	5	0	1	2	3	4

Identity

Elts. combined with identity

Modular boundary

$3 + 4 \equiv 7 \equiv 1 \pmod 6$

Modular Arithmetic and Groups

Coprime: Two numbers are coprime if and only if the largest integer they are both divisible by is 1.

$$\mathbb{Z}_6^\times = \{1, 5\}$$

$\times$	1	5
1	1	5
5	5	1

Identity

Elts. combined with identity

$5 * 5 \equiv 25 \equiv 1 \pmod 6$

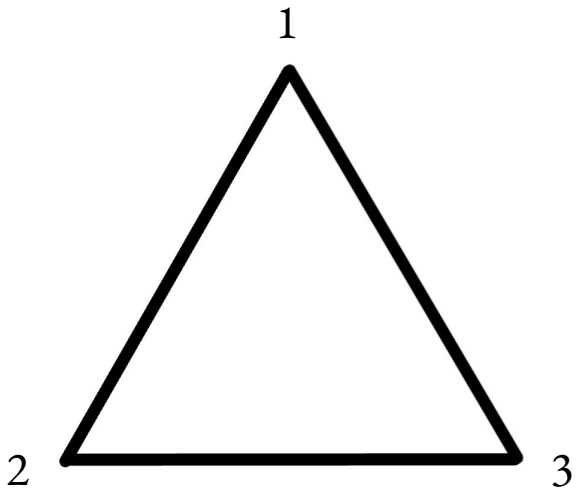
Groups? What else can you do with them?

Group Symmetries!

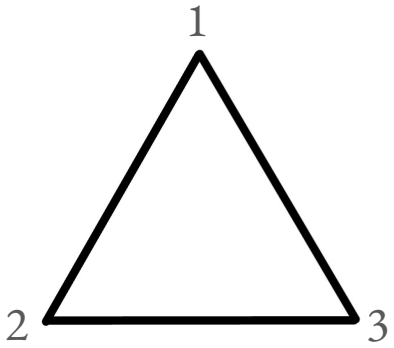
- Solve algebraic puzzles (rubik's cube)
- Analyze structure (different types of groups)

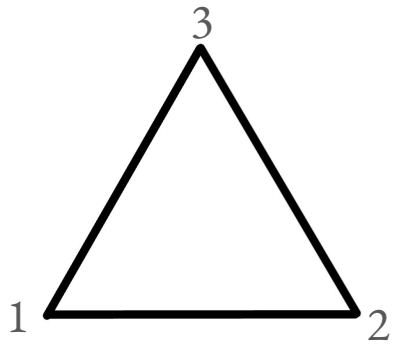
They are similar in many ways and different many others.

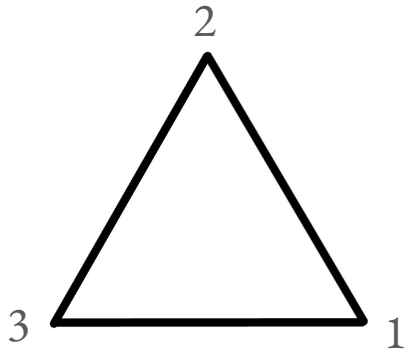
This is a Triangle.

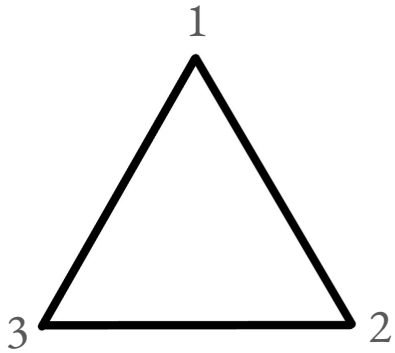


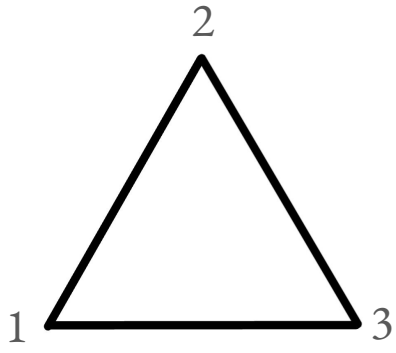
More Triangles!

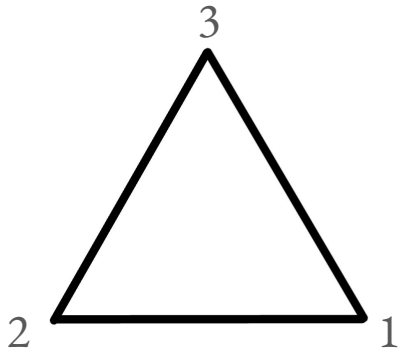




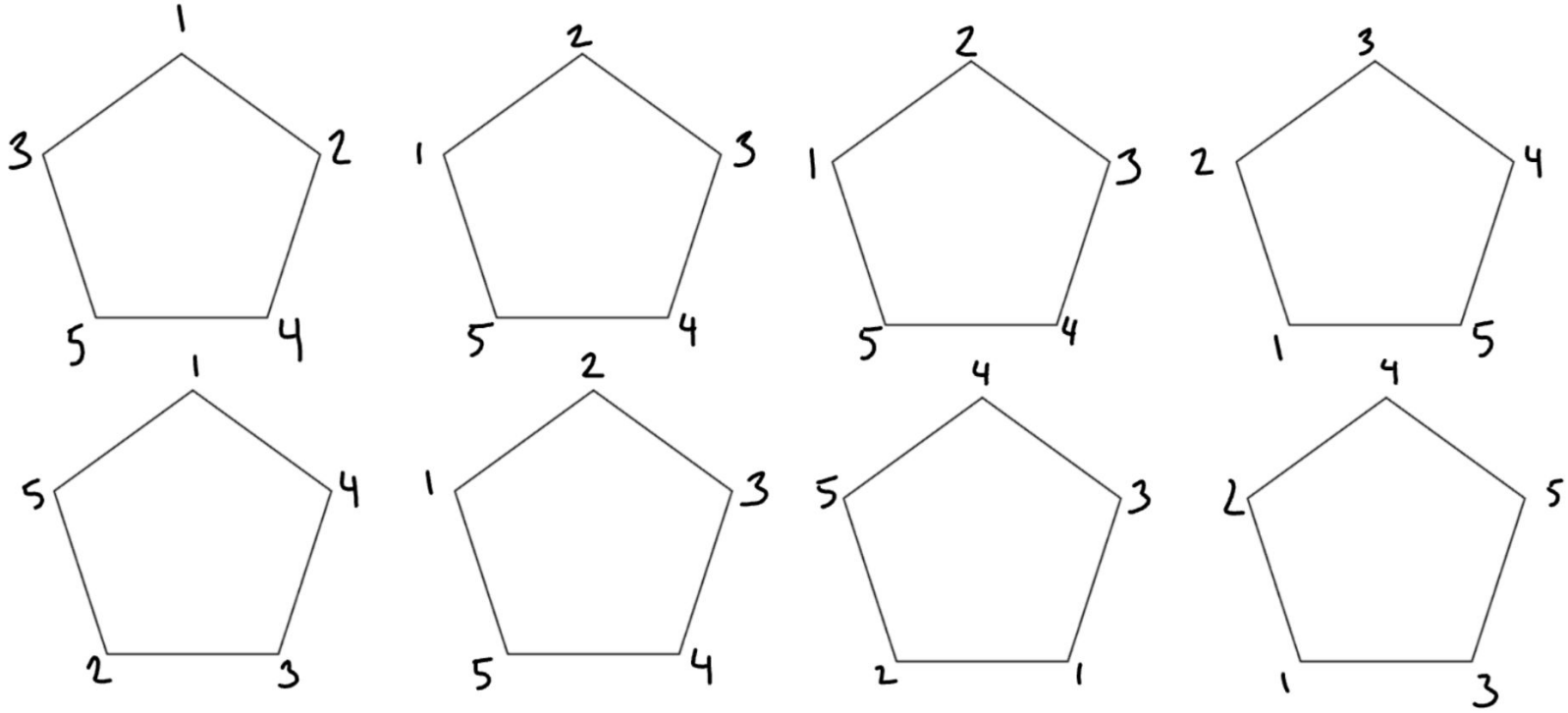








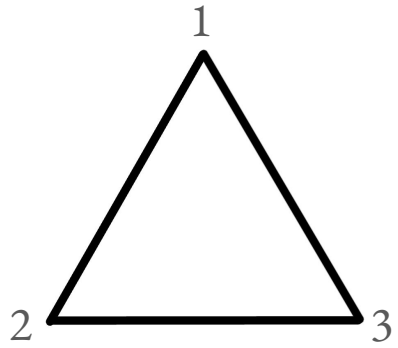
Are These The Same?

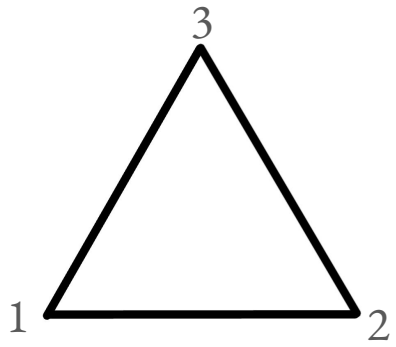


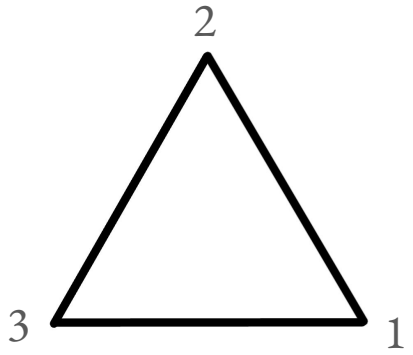
No!

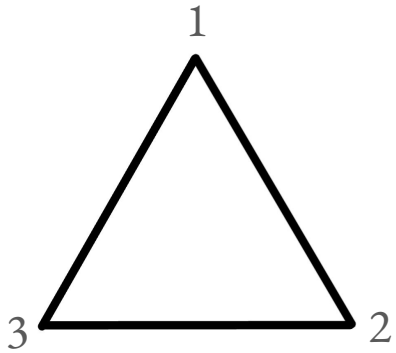
But *how* do we know this? How can we tell if two shapes are the ‘same’ polygon?

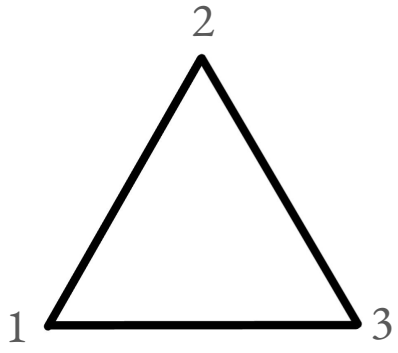
Same Triangles?

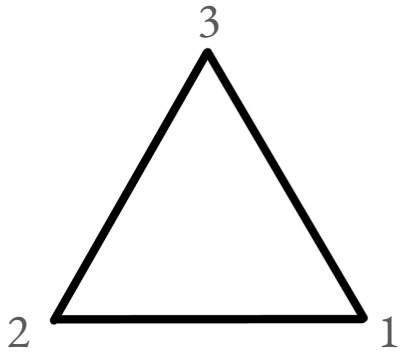




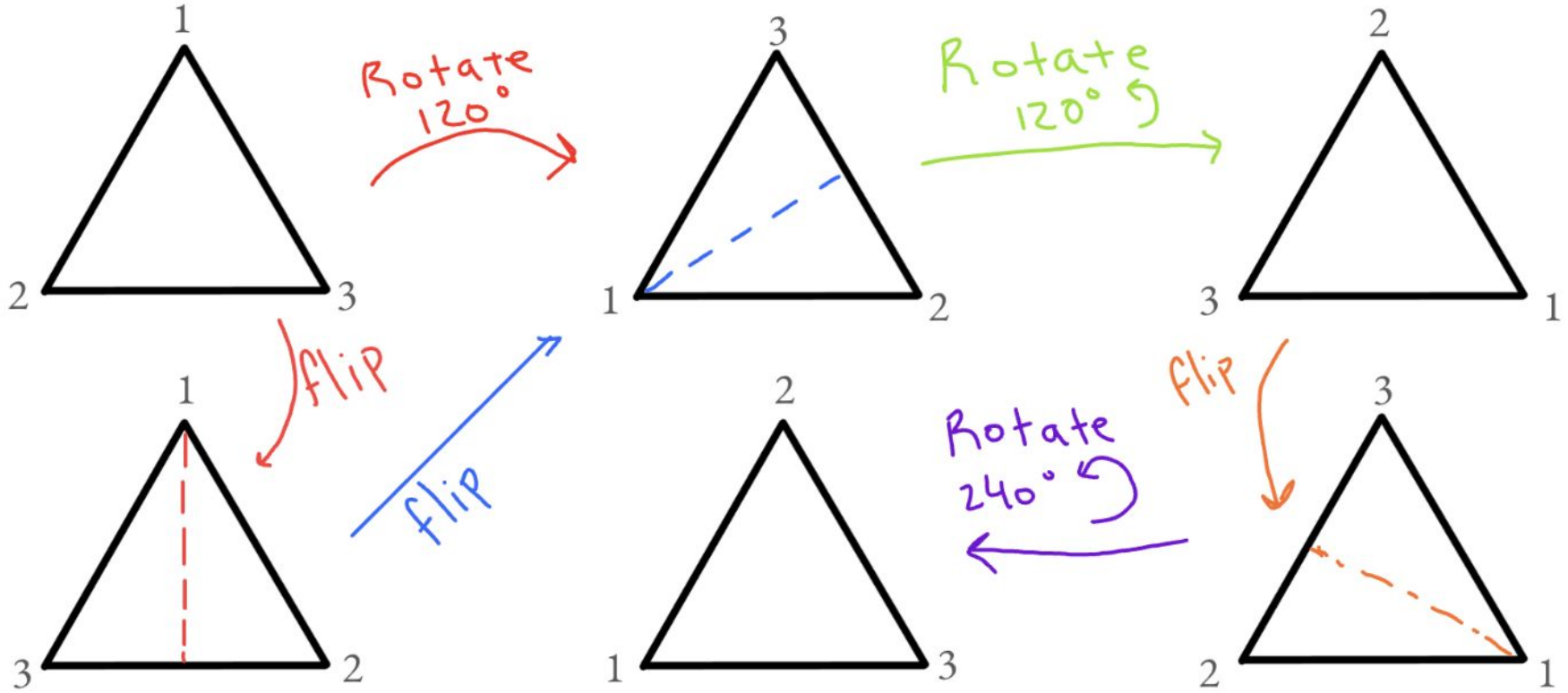








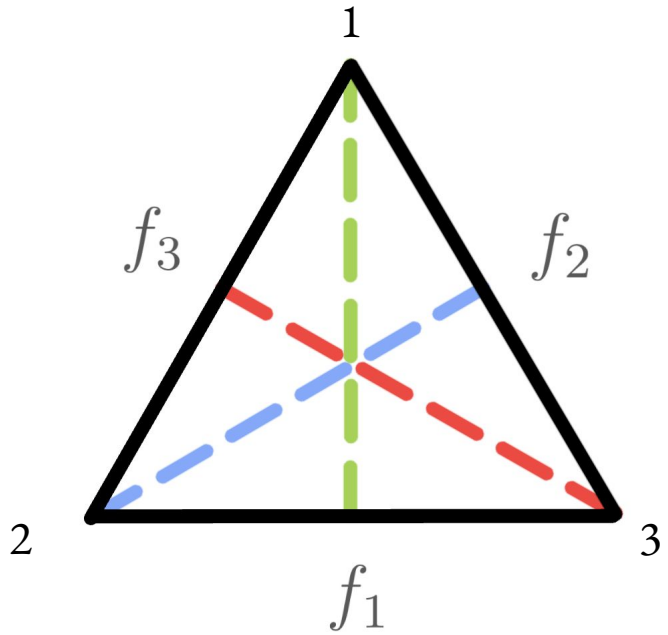
Same Triangles?— yes!



Applying Rigor...

f defines a flip along an particular axis (independent)

r defines a rotation 120 (r) or 240 (r^2) counterclockwise



Group Symmetries Satisfy Similar Axioms

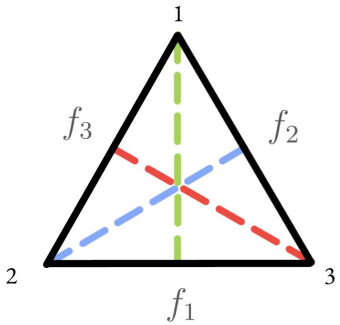
Closure: Can't find an additional element by performing known rotations or flip.

Identity: Rotating 360 or flipping on the same axis twice returns to the "starting place"; $e = r^3 = f^2$

Associativity: $A \oplus (B \oplus C) = (A \oplus B) \oplus C$

In other words, when we apply the following, we get the same triangle!

$$(r \oplus f) \oplus r^2 = r \oplus (f \oplus r^2)$$



A Computational Calculation

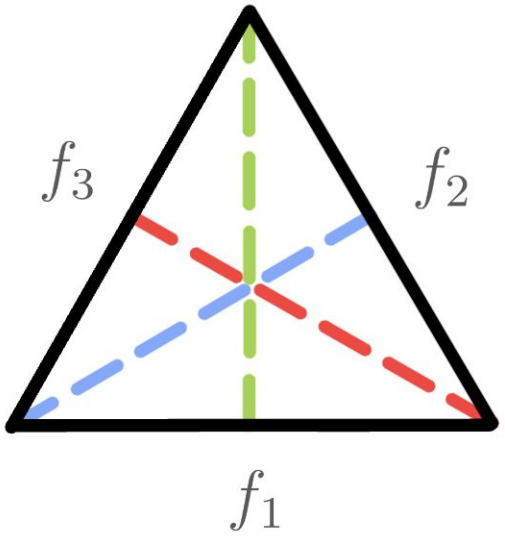
We didn't have a commutation axiom, but we can create a substitute: a commutation relation!
This tells us how *f* behaves from the perspective of someone who has rotated the world by *r*.
We can begin with:

$$(r^2 f)(r) = r^2 f r(r r^{-1}) = r^2 f r^2 r^{-1}$$

$$= r^2 r f r^{-1} = f r^2 = r f$$

We've found our commutation relation:

$$f r^2 = r f$$



$$< r, f : r^3 = f^2 = e, f r^2 = r f >$$

Many thanks to…

The MIT PRIMES Program
Our mentor, Sam
Ivan Niven, Herbert S. Zuckerman, and Hugh L Montgomery for their book *An Introduction To The Theory of Numbers*