CYCLICITY AND ORDER OF GROUPS

SAM ROVEN (ROVENSAM@GMAIL.COM)

In honor of the upcoming birthday of the great mathematician, Carl Freidrich Gauss, we are going to investigate one of the great questions that he answered as a young mathematician. We will refer to this as **Gauss' birthday question**. In order to investigate this question, we first must become familiar with some definitions and concepts involving what is formally known as a group.

ADDITION!

Let $\mathbb{Z}_n$ be the group of integers $\{0, 1, 2, \ldots, n-1\}$ under addition modulo n. In this group we refer to addition as the *group operation*, which can be changed for other suitable operations, like multiplication modulo n. Recall that to write a number $\pmod{n}$ means to write the remainder when a number is divided by n; this is is always a number 0 through $n-1$.

Example: $\mathbb{Z}_5 = \{0, 1, 2, 3, 4\}$, and addition of any two integers in $\mathbb{Z}_5$ is reduced modulo 5, so $4 + 3 = 2$, and $3 + 3 = 1$.

We are interested in several properties of this group, one being what is known as the **order of the group**. The order of the group is simply the number of elements in the group, sometimes written as $|G|$ for some group G. What is $|\mathbb{Z}_5|$?

We define a group G to be **cyclic**, if there exists one element that, when repeatedly operated on itself, creates the entire group. If a group is indeed cyclic, the elements that create the entire group are called generators, and we say that they *generate* the group.

Example: Take the element 2 in $\mathbb{Z}_5$. We can see that $2 = 2$, $2 + 2 = 4$, $2 + 2 + 2 = 1$, $2 + 2 + 2 + 2 = 3$, and $2 + 2 + 2 + 2 + 2 = 0$. Thus repeated addition of 2, modulo 5 has created all of $\mathbb{Z}_5 = \{0, 1, 2, 3, 4\}$, hence 2 is a generator of $\mathbb{Z}_5$, and $\mathbb{Z}_5$ is a cyclic group.

1. What is the order of $\mathbb{Z}_n$?
2. Aside from 2, what are the other generators of $\mathbb{Z}_5$?
3. Is $\mathbb{Z}_6$ cyclic? If so, what are its generators?
4. If p is prime, is $\mathbb{Z}_p$ cyclic? If so, how can we find all of its generators?

5. For which positive integers n is $\mathbb{Z}_n$ a cyclic group under addition modulo n? For the cyclic ones, what are it's generators?

6. What order related observations can you make about the size of the sets created by the non-generator elements in $\mathbb{Z}_n$? How do they relate to the order of the group?

7. What important role does the element 0 play in $\mathbb{Z}_n$?

<u>MULTIPLICATION!</u>

Now let's change the operation of $\mathbb{Z}_n$ from addition modulo n to multiplication modulo n. We will denote this by writing $\mathbb{Z}_n^\times$.

8. What role does the element 1 play in $\mathbb{Z}_n^\times$?

We will see in class, that the multiplication tables for $\mathbb{Z}_n^\times$ are slightly trickier than that of $\mathbb{Z}_n$. When the operation was addition, the addition table had a "nice structure". We will refer to this nice structure as the sudoku principle.

9. If n is composite, what elements are necessary for the multiplication table of $\mathbb{Z}_n^\times$ to satisfy the sudoku principle?

10. If p is prime, what elements are necessary for the multiplication table of $\mathbb{Z}_p^\times$ to satisfy the sudoku principle? What does this imply about the order of these multiplicative groups?

11. Find the following orders: $|\mathbb{Z}_6^\times|$, $|\mathbb{Z}_7^\times|$, $|\mathbb{Z}_8^\times|$. Can you see a familiar pattern?

12. If p is prime, find $|\mathbb{Z}_p^\times|$. Similarly, for a composite integer n, find $|\mathbb{Z}_n^\times|$

13. Is $\mathbb{Z}_6^\times$ a cyclic group? What about $\mathbb{Z}_7^\times$? If so, what are its generators?

To fully answer the following question, we will undoubtedly need some number theory...

Gauss' birthday question:
For what positive integers, n, is $\mathbb{Z}_n^\times$ a cyclic group?

NUMBER THEORY!

Pick a positive integer, $n \leq 10$, and list all the fractions with denominator n and numerator less than n. Now write all those fractions in lowest terms and count how many fractions you couldn't simplify. This count is known as *Euler's totient function*, written $\phi(n)$.

In more mathematical terms we say $\phi(n)$ is the number of positive integers relatively prime to n. In other words the positive integers less than n that share no common factors with n.

Euler's Totient Function
14. To warm up, find values of $\phi(n)$ for $n = 2, 3, \ldots 21$.

15. If p is a prime, what is $\phi(p)$?

16. What if we have a number that is a product of two primes, say p and q? What is $\phi(pq)$? How does this compare to $\phi(p)\phi(q)$?

17. Is it always true that $\phi(xy) = \phi(x)\phi(y)$? If not, what are the exceptions?

18. Determine a formula for $\phi(n)$ in terms of the prime factorization of n.

The Reduced Totient Function
Let $\lambda(n)$ be the smallest positive integer, m, such that $a^m \equiv 1 \pmod{n}$, *for every integer*, a, that is relatively prime to n. We call this the Reduced Totient function.

19. Find $\lambda(6)$, $\lambda(7)$, and $\lambda(8)$? (Hint: think about *least common multiples*)

20. If p is a prime, what is $\lambda(p)$? How does this relate to $\phi(p)$?

Gauss' Birthday Question Part II:
How do $\phi(n)$ and $\lambda(n)$ relate to the cyclic behavior of $\mathbb{Z}_n^\times$

SYMMETRY GROUPS!

The dihedral group, written as D_n, is the set of all rigid symmetries of a regular n-gon. We will define a rigid symmetry in class.

21. List the elements of the groups D_4 and D_5. What is $|D_4|$? $|D_5|$?

22. In general, what is $|D_n|$?

23. Is D_n a cyclic group for any positive integers n? If so, what are it's generators.

Now, fix one vertex, x, of a regular n-gon and determine the number of vertices (including itself) that it can *travel* to via rigid symmetries. We will refer to this as the Orbit of a vertex, denoted $Orb(x)$. The name orbit stems from the definition on an orbit being a curved path of an object or point in space. We can think of the orbit of a vertex as the other vertices lying on this path.

Now with the same vertex, x, count the number of rigid symmetries that leave x fixed. We will call this the Stabilizer of x, denoted $Stab(x)$. The name is useful in remembering that the stabilizer of a vertex is the set of symmetries that keep the vertex *stable*. In other words, it is the elements that do not move the vertex.

24. Find $Orb(x)$ and $Stab(x)$ for vertices of a square and a pentagon. How do $|Orb(x)|$ and $|Stab(x)|$ relate to $|D_4|$ and $|D_5|$?

25. Can we generalize this relationship to find $|D_n|$?

26. If this works in 2-dimensions can it work in 3? Try and make a similar argument for the cube and the tetrahedron. Can we apply this method to other polyhedra?