A Whirlwind Tour of Group Theory and Number Theory (Not Fair Game on Exams)

By Grayson York
A Little Bit of History

- Some debate over when the field was started, many other fields used group theory ideas before the objects were studied formally
- The term “group” was coined by Evariste Galois in the early 1800s
- In 2004, the mathematical community finished the total classification of all finite simple groups.
  - The longest mathematical proof ever written (10,000+ pages, 100+ authors)
  - Work is still ongoing to make it readable
  - One of the biggest successes of modern mathematics
- Group theory has applications to many fields including computer science, physics (the standard model), music (the circle of fifths)
What is a group?

- We will start with an example, the integers under addition.
- A group has 2 things, a set and an operation.
- The set and operation must satisfy 4 axioms:
  - The set is closed under the operation (the sum of 2 integers is an integer).
  - The operation is associative ((a+b) + c = a + (b+c)).
  - The group has an identity element (0 + x = x for every integer x).
  - Every element has an inverse (-x + x = 0 for every integer x).
- It turns out, there are a lot of groups that we encounter in the mathematical world!
The Positive Real Numbers Under Multiplication

- Is the set closed?
  - Yes! The product of two positive real numbers is a positive real number.
- Is the set associative?
  - Yes! a(bc) = (ab)c.
- Does the set have an identity?
  - Yes! 1*x = x for every x.
- Does every element have an inverse?
  - Yes! x * 1/x = 1 for every x.
- It is a group!
The Integers Modulo n Under Modular Addition

- Is the set closed?
  - Yes! When we add two numbers, then take the sum mod n, the result is an integer mod n.
- Is the set associative?
  - Yes! $a + (b + c) = (a + b) + c$.
- Does the set have an identity?
  - Yes! $0 + x = x$ for every $x$.
- Does every element have an inverse?
  - Yes! $x + (n-x) = 0$ for every $x$.
- It is a group!
The Nonzero Integers Modulo p for Prime p

- **Is the set closed?**
  - Yes! When we multiply two numbers, then take the product mod p, the result is an integer mod p.

- **Is the set associative?**
  - Yes! Because multiplication is associative.

- **Does the set have an identity?**
  - Yes! $1 \times x \mod p = x \mod p$ for every $x$.

- **Does every element have an inverse?**
  - Yes! More difficult to show, but it turns out for every $x$, there is a $y$ such that $xy = 1 \mod p$.
  - Note that when we write $y = x^{-1}$, that does not mean that we raise $x$ to the $-1$ power, just that we find the inverse somehow.

- **It is a group!**
Rubik’s Cube Positions Under Face Rotations

- Is the set closed?
  - Yes! When we make any valid set of rotations, we get a new valid Rubik’s cube position.
- Is the set associative?
  - Yes! A bit more difficult to visualize, but it is associative.
- Does the set have an identity?
  - Yes! The lack of any rotations keeps the cube the same.
- Does every element have an inverse?
  - Yes! We can do any combination of rotations backwards to get back the cube with no rotations.
- It is a group!
The Integers Between 5 and 10 Under Addition

- Are the integers between 5 and 10 a group under addition?
- What if we add 7 and 8?
  - Not an integer between 5 and 10!
- Does it have an identity element?
  - No! 0 is not in this group!
- Does it have inverses?
  - No! There are no negative numbers in the group!
- We only needed to fail one test to not be a group, but we have failed 3!
- Not a group!
What is a Subgroup?

- A subset of a group which is also a group
- Imagine the even integers, a subgroup of the integers under addition
  - Sum of 2 even integers is an even integer
  - Still associative
  - Contains 0
  - If x is even, -x is even
- Are the odd integers a subgroup?
  - No! 0 is not odd, so there is no identity
The Powers of $x$ Modulo $n$

- Are the powers of $x$ Modulo $n$ for $x$ relatively prime to $n$ a subgroup of the nonzero integers modulo $n$ under multiplication?
- Is the set closed?
  - Yes! $x^a x^b \mod n = x^{a+b} \mod n$, also a power of $x$ modulo $n$!
- Is the set associative?
  - Yes! Multiplication is associative
- Does the set have an identity?
  - Yes! $x^0 = 1 \mod p$
- Does every element have an inverse?
  - Yes! $(x^{-1})^a$ is the inverse of $x^a$
- This is a subgroup!
A particularly interesting class of subgroups

- What about the even integers mod 12?
  - The sum of 2 even integers mod 12 is an even integer mod 12
  - Still associative
  - 0 mod 12 is even
  - If x mod 12 is even, 12 - x mod 12 is also even and x + 12 - x = 12 = 0 mod 12
  - This is a subgroup!

- We can think of this as all the integers in the form 2x mod 12

- Under what conditions on k,n are the integers of the form kx mod n a subgroup?
  - Any time that k divides n, these integers will be a subgroup
Lagrange’s Theorem

- The most important result in all of group theory
- The size of every subgroup must divide the size of the larger group
- As a corollary, the length of any cycle must divide the size of the group
- As another corollary, a group whose size is a prime can only have a cycle if it touches the whole group
- This might be starting to look familiar...
Open Address Probing Sequences

- What if we build the open addressing scheme \( h(x,i) = h_1(x) + i h_2(x) \mod n \)?
- What if we thought of the subgroup of multiples of \( h_2(x) \)?
  - How large would this group be?
  - If we wanted to make this group as large as possible, \( h_2(x) \) should not divide \( n \)
  - Hopefully this sounds like a best practice from the slides on hashing
- What happens if the subgroup is very small?
  - The subgroup is closed under addition!
  - No matter how large of an \( i \) we choose, we will always get the same table entries as the multiples of the subgroup entries will also be in the subgroup
Number Theory!

- The study of the properties of numbers e.g. primes
- One of the oldest branches of math
- Surprisingly interdisciplinary within the math world, uses group theory, field theory, even complex analysis
- Very important applications to cryptography
A Motivating Question, Primality Testing for RSA

- The first step of RSA involves finding 2 large primes
- How can we tell if an n bit number is prime?
- There are $2^n$ possible divisors, so testing all of them is infeasible
- Being a bit more clever, we can just try $2^{n/2}$ divisors, still infeasible
- Can we make a test that does not involve testing divisors?
Another Motivating Question, Modular Inverses for RSA

- Given a number a and prime p, we know that there is some b such that \( ab = 1 \pmod{p} \)
- how do we find b?
- If p has n bits, then brute force requires trying \( 2^n \) possibilities
- Can we do better?
Fermat’s (Little) Theorem

- A very useful result for studying primes
- NOT THE SAME THING AS FERMAT’S LAST THEOREM
  - That one involves generalizations of the pythagorean theorem
  - That will not be covered in this class
- For a prime $p$, $a^{p-1} = 1 \mod p$
- A very surprising result, what tools could we use to prove it?
Proof Using Group Theory and Lagrange’s Theorem

- The nonzero integers modulo p are a group under multiplication!
- The powers of an element a are a subgroup of the nonzero integers modulo p.
- Multiplication by the element a must cycle us through all of the elements of the subgroup, as all powers of a can be reached by doing this.
  - We see that if \( a^i = a^j \), then \( a^{i+1} = a^{j+1} \) and so on
  - Therefore, once one element repeats, all the elements must repeat
- Notice that 1 must be in the subgroup, and \( 1 \cdot a = a \)
- Therefore, 1 must be the last element in the cycle, because after we reach 1, the cycle repeats starting with a
- That is, if the cycle has length k, \( a^k = 1 \)
More Proof Via Lagrange

- If the cycle has length $k$, $a^k = 1$
- Using Lagrange's theorem, what is the size of the subgroup of powers of $a$?
  - Must divide $p-1$ because there are $p-1$ nonzero integers mod $p$
- Therefore, $p-1 = hk$ where $k$ is the length of the cycle and $h$ is some integer
- Recall that $a^k = 1 \text{ mod } p$
- Therefore $a^{p-1} = a^{hk} = (a^k)^h = 1^h = 1 \text{ mod } p$
Let’s Look at Some Examples

- Each of the above a values is chosen arbitrarily, and each p value is prime
- Each time, we get 1, as predicted by Fermat’s theorem
- Good news, the theorem works!
Can We Use This To Calculate Inverses mod P Quickly?

- What if, given a number $a$ and prime $p$, we want to find $a^{-1} \mod p$, can we do it quickly?
- If $a^{p-1} \mod p = 1$, then $a \cdot a^{p-2} \mod p = 1$
- Therefore, $a^{-1} = a^{p-2}$ as they are two numbers that multiply to 1
- We can calculate $a^{p-2}$ in $O(\log p)$ multiplications using repeated squaring!
- If $p$ has $n$ bits, then $\log(p) = O(n)$
- This is a critical step in calculating RSA keys
Can We Use This to Test Primality?

- We know that if $p$ is prime, then $a^{p-1} = 1 \mod p$, but is this true in the other direction?
- If $a^{p-1} = 1 \mod p$, then does that imply that $p$ is prime?
- Unfortunately the answer is no
- Numbers like 341 are called pseudoprimes or Carmichael numbers

```python
>>> 11*31
341
>>> (2**340)%341
1
```
Is There Any Hope?

- Let’s try some other numbers mod 341:
- Informally it looks like 1’s are rare
- What if we try a Monte-Carlo approach?
The Miller-Rabin Primality Test

- It turns out that if \( p \) is composite, the probability that \( a^{p-1} = 1 \mod p \) is at most \( \frac{1}{4} \).
- Therefore, if pick \( k \) random \( a \) values, \( a_1, a_2, \ldots, a_k \), and for every \( i \), we get \( a_i^{p-1} = 1 \mod p \), then the probability that \( p \) is composite is at most \( \frac{1}{4^k} \).
- Because each Fermat test can be run so fast, we can easily make this probability negligible by running the test many times.
Can We Do Even Better?

- Not really, Miller Rabin is usually used in practice
- Gary Miller’s original test, on which Miller Rabin was based was deterministic
  - The test cleverly chose a set of a values which always works
  - Unfortunately, the correctness proof relies on the Riemann Hypothesis
  - The Riemann Hypothesis is almost as significant an open problem as P vs NP
- Pomerance et al. use a more complex primality test (1980)
  - Foiled by Lucas numbers, which are far rarer than Carmichael numbers
  - More difficult to compute in practice
- Agrawal et al. found a deterministic polynomial test (2003)
  - Does not rely on unproven hypotheses
  - Involves a very complex test
  - Too slow to be practical