A Peek Into Number Theory

Muhammed Yaseen

"Mathematics is the queen of the sciences and number theory is the queen of mathematics."
—Carl Freiderich Gauss

1 Introduction

Everyone knows at least something about numbers. Some know a lot more than others, while others are happy with what they know. Numbers are ubiquitous. They seem to be part of the foundations of the universe. They can, quite accurately, describe the universe. But what about the numbers themselves? How do they behave? If I showed you the following equation

$$x^n + y^n = z^n$$

and asked you to solve for x, y, z, when n is fixed at a particular value, you would be quite baffled. And I wouldn't blame you for that! That equation took mathematicians 3 centuries to solve! Today, it is known as Fermat's last theorem. Pierre de Fermat was a french mathematician and lawyer. His 'little theorem' is revered by math olympians across the world. He stated the following:

For $n > 2$, the equation $x^n + y^n = z^n$ has no values of x, y, z that satisfy it.

The only issue was that he did not provide a proof. And as is the case for any mathematical statement, it is always considered false unless proven. But the plot thickens, Fermat claimed he knew the proof! According to him, the margin of the notebook he wrote the theorem in was too small. And thus began the 300-year old journey to find a proof. It was finally solved in 1994 by British mathematician Andrew Wiles.

Thus, we can think of number theory as the study of integers themselves.

2 Prime Numbers

Primes have intrigued humanity for a long time now. You might tell me that a prime is a number with only 2 factors, 1 and the number itself. That is true. To get a more tangible idea about primes, we play a small game.
In how many ways can you group 7 balls, given the condition that you can't cut any ball and that you can use as many bags as you want but all of them must contain the same number of balls?

First, let all bags contain 1 ball. Then by simple logic, we will require 7 bags. So that's the first way. Is there any other method? If we ponder for a while, we could let all of the balls be in 1 bag. So that's the second way. Cool. But is there any other way? The answer is no. You can try all you want, but as long as our 2 conditions hold, there will only be 2 ways to group these 7 balls. If we use mathematical notation to represent these scenarios, we get

$$7 = 7 \times 1 \qquad \text{7 bags of 1 ball each gives us 7 balls in total}$$

$$7 = 1 \times 7 \qquad \text{1 bag of 7 balls each gives us 7 balls in total}$$

Apparently, if you repeat this game with, instead of 7, 3 balls, or 11 balls or 13 balls or 59 balls, there will only be 2 ways to group the balls (similar to the grouping we observed for 7). These numbers, which can only be grouped in two ways are called prime numbers.

From this, we can understand that prime numbers.... just exist. An interesting point is that the smallest and only prime is 2. Hmmm... We know that there are infinitely many numbers. But are there infinitely many primes? Intuitively, one might say yes. We know it as a fact. But how did the mathematical pioneers establish this? That requires the next section.

3 Divisibility of Integers - The Backbone of Number Theory

3.1 Basic Results

Firstly, let us define the term 'multiple' to be the number that is the product of two (or more) numbers. Similarly, we define a factor of a number,to be the number, that upon dividing the number by it, the remainder turns out to be 0. Factors are also called divisors, and the two terms are interchangeable. With that out of our way, we define a number to be divisible by another number if it is a factor of the second number. Conversely, if a number is a multiple of another number, then the second number is a factor of the first. From this, we can infer that

$$\text{Product of Factors} = \text{Multiple}$$

To make math more easier to write, mathematicians have agreed to use the symbol $|$ to say 'divisible by'. For example, if we write $a \mid b$, this means that b is divisible by a. From our discussion, we can also see that, if $a \mid b$, then $b = ak$, for some integer k. k cannot be a fraction, but it can certainly be negative. Think about it. We know that $5 \mid 30$. And we definitely can write $30 = 5 \times 6$. But what if $a \mid b$ *and* $b \mid a$? That is for you to figure out. Another trivial fact is that $1 \mid n$ and $n \mid 0$ for any integer n.

3.2 The Fundamental Theorem of Arithmetic

Number theory is incomplete without The Fundamental Theorem of Arithmetic.

> The Fundamental Theorem of Arithmetic:
>
> Any integer greater than 1 can be expressed as the product of primes.

Although as budding mathematicians, we demand proofs, the proof of this theorem is simply beyond the scope of this article. If you read it properly, you would recognize the 'theorem' to be nothing other

than the fact that any number can be expressed as the product of its factors! Sometimes, mathematicians like to make simple concepts sound huge, and only upon closer inspection does one actually see that there is nothing very hard about it! Let us verify the theorem for some small numbers. Take for example, 210. You could say that

$$210 = 21 \times 10$$

But they aren't prime numbers. Have we found a counterexample to the theorem? The answer is no, because we can break up 21 and 10 further to get

$$210 = 3 \times 7 \times 2 \times 5$$

And indeed, we see that the fundamental theorem of arithmetic holds for 210. Why don't you try it for 1800?

3.3 There Are an Infinite Number of Primes

Now that we have looked into the FTA, we can go back to our question: Are there infinite primes? Euclid said yes, and provided the following proof.

Assume that there are k number of prime numbers $p_1, p_2, p_3, p_4, ..., p_k$. Let N be the number given by

$$N = p_1 p_2 p_3 p_4 ... p_k$$

Since there are infinite numbers, $N + 1$ definitely exists. Then

$$N + 1 = p_1 p_2 p_3 p_4 ... p_k + 1$$

Then, by FTA, $N + 1$ must have some sort of a prime factorization. But since the only primes that we know of $(p_1, p_2, p_3, p_4, ..., p_k)$ are all coprime to $N + 1$, we cannot express $N + 1$ as a product of primes. Therefore, the assumption that only a finite number of primes exists is wrong. Therefore, an infinite number of primes exist.

4 Euclid's Divison Lemma

The name might have, perhaps, scared you. Let us look at a simple problem. Consider $22 \div 7$. What is the quotient (q) and remainder (r)? Doing some long division, we get $q = 3$ and $r = 1$. How can we express 22 in terms of q and r? After some thought, we see that

$$22 = 3 \times 7 + 1$$

If this concept looks familiar, it is no coincidence! All we did was use the fact

$$\text{Dividend} = \text{Divisor} \times \text{Quotient} + \text{Remainder}$$

But as budding mathematicians, we will always try to frame a statement that is true for all integers.

Euclid's Division Lemma

For any two integers a, b, there exist unique integers q, r satisfying

$$b = aq + r$$

where $0 \leq r < a$

If you've been reading carefully, this statement should make sense. But let us go over the condition mentioned at the end, the one that stated $0 \leq r < a$. Now, think about it: if you divide a number k by another number m, what is the largest remainder you are going to achieve?

Problems to Try

Problem 1: Is the sum of the first 3 natural numbers divisible by 3? What about the first 10 natural numbers? What can you say about the first n natural numbers? Why or why not?

Problem 2: We have looked at Fermat's Last Theorem. Which stated that for $n > 2$, there are no values of x, y, z for the equation $x^n + y^n = z^n$ (x, y, z, n are all natural numbers). Assuming that there are an infinite number of pythagorean triplets, why did we have to state the condition $n > 2$. (Hint: try plugging in different values for n, but don't forget to plug in relevant values!)

Problem 3: For some integer n, can $n + 1$ be divisible by n? Why or why not?

Problem 4: What is the remainder when $2^k + 1$ is divided by 2. ($2^k = \underbrace{2 \times 2 \times 2 \times \cdots \times 2}_{k \text{ times}}$)

Problem 5: A Mersenne prime is a prime number of the form $2^m - 1$. Find a composite number that can be expressed this way. (Hint: It's not too big)

Problem 6: We know that the smallest prime is 2. But why is it the only even prime?

Problem 7: Explain why $22221 \times 290129384396$ and 26×6 have the same unit's digit. (Hint: Distributive property)

Problem 8: Prove that if $a \mid b$ and $b \mid a$, then $a = b$ or $a = -b$. (Hint: Let $b = ak$ for some **integer** k)