Elementary Number Theory : §0

Henry Slayer | University of California, Santa Cruz

Introduction

Number Theory is the study of the integers, and their wondrous, infinite realms of complexity.

Number Theory is also the study of rational numbers, too, which we can manipulate and explore as ratios of integers. For the most part, however, we'll be looking at whole numbers, and how these whole numbers interact with each other.

Some of the results in Number Theory have a reputation for being "easy to state, hard to prove."

While I've found this to be true, I think that it's a bit short-selling. On the surface, yes, it is easy to assemble statements about arithmetic, but those simple statements often conceal beautiful, and deep relationships about the structure of numbers themselves. For what is a number? Prime, composite, solitary... these are terms that we attribute, classifications that we make, but the beauty of Number theory goes beyond this framework. Number Theory is the process of getting to know numbers as personalities, objects and beings unto themselves. Number theory breathes life into these simple objects, and gives us tools for exploring their many ways of interacting and playing with each other. In my opinion, there's a real elegance to number theory that wears well. Working with the integers has brought me a certain simple and curious satisfaction. And by simple, I don't mean lacking in complexity. Number theory affords as much complexity as one wants to give it. Analytic techniques from real and complex analysis have completely re-shaped the way that we look at the humble whole number. We can investigate entirely new number systems, such as the Gaussian and Eisenstein integers, which can be applied to the exploration of topics such as cubic reciprocity. And, the applications of Number Theory in the 'real world' have some teeth. Number theory has powerful, practical applications from data security to algorithm design to scientific computing. Elementary Number theory is a rich subject, and many other branches of mathematics can be traced to its origin. Elementary number theory is responsible for the birth of the complex variable, the development of algebraic and analytic number theory, and some of the most powerful insights into the nature of numbers themselves.

> Matters of mind aside, elementary number theory is a great place to fall in love with mathematics. I would say that my first number theory course inspired that little whisper in the back of my brain... *I think that I could do this for a lifetime.* Even if number theory isn't your cup of tea, it does provide a solid foundation for further study in mathematics, especially for those who are new to writing proofs and thinking mathematically. My hope is that in whatever extent you engage with number theory, it can afford you one or both of these wonderful benefits.

These series of articles are based on an undergraduate number theory course that I took in the spring of 2019. I would say that my experience was made by a great professor and a great text, two influences that will be present (either explicitly or implicitly) in all of the writing that follows. I would like to thank Edmund Karasiewicz for his fantastic instruction in the course, and the wonderful guidance provided by Martin Weissman's text *An Illustrated Theory of Numbers*. If you are interested in learning more about this book, visit

`http://illustratedtheoryofnumbers.com/`

My intention moving forward in this series is to present the fundamental ideas of Elementary number theory, using proofs inspired by Weissman's methods, as well as the work of other mathematicians such as Erdos and Rosen. Any mistakes or errors are of my own doing. Above all else, my intention is to produce a readable and enjoyable journey through the theory of numbers, and to provide the reader with a solid foundation for further study. The prerequisites for understanding the material aren't much: high school math through pre-calculus, all the better if the reader has taken an introductory proofs course, or something similar. At any rate, if anything feels confusing, you're probably on the right track.

Take heart. You're beginning on a mathematical journey that's been unfolding since the time of the ancient Greeks, and even before then. Welcome to the theory of numbers.

Our Universe: Z, N, Q

For the majority of what's to come, we'll be working with whole numbers, or fractions of whole numbers. These include the integers ($\mathbf{Z}$), the natural numbers ($\mathbf{N}$), and the rational numbers on occasion ($\mathbf{Q}$).

$$\mathbf{Z} = \{\dots, -2, -1, 0, 1, 2, \dots\} \qquad \mathbf{N} = \{0, 1, 2, 3, 4, \dots\} \qquad \mathbf{Q} = \{\frac{a}{b} : a, b \in \mathbf{Z}\}$$

The integers are the infinite set of whole numbers ranging from $-\infty$ to ∞. The natural numbers are the collection of nonnegative integers, and the rational numbers are fractions of integers. For now, though, we'll put rational numbers on the back burner and consider some of the basic principles of integers and natural numbers.

Basic Principles: Divisibility

One of the first questions that we can ask about numbers is how they go into each other. Divisibility between two numbers always implies that there's a third party. We say that an integer a divides b if there exists another integer x such that $ax = b$. We can divide b into x chunks, where each chunk is the size of a. Another way to say this is that b is a multiple of a. We denote divisibility by $a \mid b$.

$$\boxed{a \text{ divides } b} \quad \Leftrightarrow \quad \boxed{a \mid b} \quad \Leftrightarrow \quad \boxed{ax = b} \quad \Leftrightarrow \quad \boxed{b \text{ is a multiple of } a}$$

Divisibility comes with some implications and intuitions. First of all, if a divides some other number b, b can't be smaller than a. So, $a \mid b$ implies $a \leq b$. Second, suppose that $a \mid b$ and $a \mid c$. And then, suppose that b and c sum to some other number, d. That is, $a \mid b$, $a \mid c$, and $b + c = d$. Then, it naturally follows that $a \mid d$.

The principle above comes in handy in all sorts of ways.

Basic Principles: GCD and LCM

We end this introduction with two definitions, which we will return to frequently. Divisibility encourages us to define two special numbers, both related to each other, and related to the integers that define them.

We define the **greatest common divisor** of two integers a and b to be another integer, g. g has some special properties that make it the greatest common divisor. First, $g \mid a$ and $g \mid b$. This is the common part of the definition. Secondly, if a and b have any other common divisor(s), say d, then $d \mid g$. That is to say, among all of the common divisors of a and b, g is the greatest.

The **least common multiple** is the greatest common divisor's kid brother. The least common multiple of two integers a and b is an integer l. l has the property that both $a \mid l$ and $b \mid l$. That is, l is a common multiple of both a and b. Furthermore, for any other common multiple of a and b (some other integer m such that both a and b divide m), l is a divisor of m (*i.e.* $l \mid m$). So, among all of the common multiples of a and b, l is the smallest.

Greatest Common Divisor:
Let a and b be integers. Then, the greatest common divisor, $GCD\,(a, b)$ is another integer g such that

(i) $g \mid a$ and $g \mid b$

(ii) For any other integer d, where $d \mid a$ and $d \mid b$, then $d \mid g$.

Least Common Multiple:
Let a and b be integers. Then, least common multiple, $LCM\,(a, b)$ is another integer l such that

(i) $a \mid l$ and $b \mid l$

(ii) For any other integer m, where $a \mid m$ and $b \mid m$, then $l \mid m$.

Exercise. *Let a, b, c be positive integers. Prove that*

$$GCD\,(a, GCD\,(b, c)) = GCD\,(GCD\,(a, b), c)$$

And then, state and prove a similar result for the LCM.

(Hint: if $a|b$ and $b|a$, then $a = b$)
(Source: [MW] p.44)

Exercise. *Suppose that a, b, q, r are integers, and $a = q(b) + r$. Let g be a nonnegative integer. Prove that*

$$g = GCD\,(a, b) \quad \text{if} \quad g = GCD\,(b, r)$$

(Source: [MW] p.31)

Exercise. *Think about the set $S = \{z : z = 2x + 3y \quad x, y \in \mathbf{Z}\}$. What do elements of this set look like? If the set-builder notation is unfriendly, consult the* ***Back Matter****.*