Chapter 6

Number Theory

"A problem in number theory is as timeless as a true work of art."
– David Hilbert

"Number theorists are like lotus-eaters - having tasted this food they can never give it up."
– Leopold Kronecker

Many find it strange to combine the words "Number" and "Theory." After all, most people think there's nothing new or theoretical about numbers, that they're entirely understood. This couldn't be further from the truth, of course, and in this chapter we set up the basic tools mathematicians and computer scientists use to understand (and pursue new ideas about) *numbers*.

You'll notice some truly ancient names popping up in our discussions, particularly *Euclid*, a fact that underscores the long-lasting appeal *numbers* hold over we mere mortals; we've literally been obsessed with understanding these things for millennia. Perhaps you, too, will fall prey to this fixation, wondering why simple-sounding questions about numbers and their abstract properties remain unsolved. Questions like "Are there infinitely many primes of the form n^2+1?" or "Are there infinitely many perfect numbers?" have resisted centuries of scrutiny and exploration.

Moreover, many Number Theory related questions require or greatly benefit from the assistance of Computer Scientists, and, conversely, a grasp on the basics of Number Theory is essential to progress in Computer Science.

The introduction to Number Theory we provide here concerns naturals, $\mathbb{N}$, and integers, $\mathbb{Z}$, as well as a lot of the structure those sets posses. We will continue to assume familiarity with adding, subtracting and multiplying, and we will rely on our previously defined notions of **divides, multiples** and **primes**.

1. Division Algorithms

You probably learned a "division procedure" back in Elementary School, one called "long division" that uses funny notation like the symbol "$\overline{)\quad}$."

Another word for a carefully sequenced "procedure" is an **algorithm**, and the "long division algorithm" you used way-back-when was based on both *grouping* and our base-10 decimal system. Calvin J. Irons' 1981 article "*The Division Algorithm: An Alternative Approach*" discusses this in accessible and easy-to-teach ways.

There are many algorithms that both help us calculate how and understand what it means to divide two integers, and the notion of *grouping* together numerical quantities plays a role in most. For example, when we write $57 \div 3 = 19$, we can read it as a claim that "3 groups of 19 make up a total of 57."

Some other Division Algorithms include the Rectangle Algorithm, the Repeated Subtraction Method, the Chunking Method, and the Big 7 Algorithm. You'll note that these algorithms overlap in various ways, and they are great items to both as refreshers *and* for any readers interested in teaching mathematics.

The Division Algorithm. Pathetically enough, what mathematicians and computer scientists refer to as ***THE** Division Algorithm* is NOT an algorithm at all! It is not a procedure comprised of carefully sequenced instructions designed to accomplish some task – it is, rather, a *mathematical theorem*! And here is what it says:

Theorem 6.1 (**The Division "Algorithm"**). *Let $a, b \in \mathbb{Z}$ with $b \neq 0$.*

$$\exists\, !\, q, r \in \mathbb{Z},\ a = q \cdot b + r$$

where $0 \leq r < |b|$.

Kind of both underwhelming *and* somewhat complicated-looking, huh? Don't worry. Pretty much *everyone* has that reaction when they first read this formal version. The following bullet points should help clarify *what* this is saying and how it relates to dividing integers.

- The equation part, $a = q \cdot b + r$, is the result of trying to divide a by b. In other words, the Division "Algorithm" tells us what will always happen when we attempt to compute a/b.
- For example, if we attempt to compute $22/4$ we find we can write $22 = 5 \cdot 4 + 2$.
- The integer q is called the "**quotient**" and **r** is called the "**remainder.**" Both values are unique (provided we are only allowing the value of r to be positive and less than $|b|$).
  - In the example above, the quotient is $q = 5$ and the remainder is $r = 2$
  - When the remainder $r = 0$, it follows that a is a multiple of b. Or, if you prefer, that $b|a$.

The Division "Algorithm" is a theorem that acknowledges a simple fact, namely that *the non-zero integers, $\mathbb{Z}^* = \mathbb{Z} - \{0\}$, is **not** closed under division.* We mathematicians tend to handle this in a couple of different ways. Sometimes we simply allow ourselves to work in the larger set, $\mathbb{Q}^*$, which *is* closed under division, but

in other situations we attempt to keep all of our computations restricted to the land of integers by using *remainders*. This second approach is appropriate when focusing on whole numbers like $\mathbb{N}$ and $\mathbb{Z}$, the way Number Theorists like to do.

So, sure, we could write $22/4 = 11/2 \in \mathbb{Q}$, but to keep everything whole-number-related, it's better and more useful to write $22 = 5 \cdot 4$ plus a remainder of 2. In other words, 22 is not a multiple of 4 – but, according to the Division "Algorithm," it is "2 units away" from being one.

Example 1.1. *Use the Division Algorithm to identify the quotient, q, and remainder, r, for each pair of integers a and b.*

(1) $a = 100, b = 8$ $(q = 12, r = 4)$
(2) $a = 8, b = 100$ $(q = 0, r = 8)$
(3) $a = 2600, b = 13$ $(q = 200, r = 0)$
(4) $a = -44, b = 3$ $(q = -15, r = 1)$

Example 1.2. *According to the Division "Algorithm," is it possible to have a remainder whose value is $r = -3$?*

Example 1.3. *According to the Division "Algorithm," if an integer a is divided by the integer 8, is it possible to have a remainder whose value is $r = 9$? What about $r = 10$? Which remainder values* are *possible?*

Why Is the Division "Algorithm" True? (i.e. What's the Proof?) If you are not too interested in the *why* of the Division "Algorithm," then feel free to skip this sub-section (perhaps this statement seems intuitively clear to you, especially having worked through our examples).

If you *are* interested in how one might prove the Division "Algorithm," then you're in luck! At least, sort of! It turns out that our Well Ordering Principle is the key ingredient in explaining our "Algorithm," but we will only provide the outline or broad strokes here.

Proof Outline for the Division "Algorithm"

(1) Given $a, b \in \mathbb{Z}$ with $b \neq 0$ form the set $R_1 = \{a - x \cdot b : x \in \mathbb{Z}\}$
(2) Form the set $R = R_1 \cap \mathbb{N}$
(3) Argue that $R \neq \emptyset$
(4) Use the Well-Ordering Principle to conclude that R contains a minimal element – this element will be the remainder r.
(5) There must exist a value of $x \in \mathbb{Z}$ so that $r = a - x \cdot b$. Label this value q.