CHAPTER I: PRIME NUMBERS

Section 1: The Building Blocks of Numbers

We begin this set of notes with a potpourri of topics that should be familiar to most readers. We will be studying numbers, and specifically the structure of various collections of numbers. Since the earliest days of mankind, numbers have fascinated people. In fact, evidence suggests that man has had the ability to count long before he could write, farm, or build. Even though scientists speculate that man has existed for hundreds of thousands of years, it was not until fairly late in our development as a species that we created civilization. Tools, the alphabet, money, and farming are all thought to be developed around the same time, roughly 4000 BC to 5000 BC. However, in 1937 a wolf's bone was found in the former Czechoslovakia that had evidence of counting dating from 30,000 BC. On this bone were 55 notches, arranged by fives, in two groups (one containing 35 notches, the other 20). Approximately 25,000 years before man was writing, he was counting.

Mathematics, however, is much more than counting. Mathematics as an intellectual endeavor developed roughly along with language and writing. The first mathematical activities were counting, measuring, surveying, and building. But that is not to say that early man did not have an interest in abstract mathematics. Evidence of Pythagorean triples, factoring, and even equation solving is found on a Babylonian tablet (named *Plimpton-322*) dated around 1600 BC. Even through this period though, numbers were utilized for other purposes. They did not "exist" in their own right.

Eventually, numbers in the abstract did become understood. Over the years people have been captivated by various properties of numbers. Perfect numbers (such as 6, 28, and 496), triangular numbers (such as 1, 3, 6, and 10), and transcendental numbers (such as π, e, and $2^{\sqrt{2}}$) are just a few examples of classifications of numbers mankind has developed over the years. There are many famous mathematicians whose main claim to fame is their dexterity with numbers. Paul Erdös, Carl Gauss, and Srinvasa Ramanujan are just three that come to mind. G. H. Hardy often told a humorous anecdote about Ramanujan,

> *I remember going to see him once when he was lying ill in Putney. I had ridden in taxi-cab No. 1729, and I remarked that the number seemed to me to be a rather dull one, and I hoped it was not an unfavorable omen. "No," he reflected, "it is a very interesting number; it is the smallest positive number expressible as the sum of two cubes in two different ways.*

This fascination with numbers in the abstract and their properties began with the Greeks around 500 BC. The Pythagoreans in general were infatuated with numbers and their properties. They classified numbers in many different ways: geometrically (triangular, square, pentagonal, etc.), arithmetically (rational and irrational), and mystically (perfect, abundant, and deficient).

Fundamental to all of these types of classification is the idea of factoring. Those numbers that cannot be factored are our focus in this section.

Definition 1.1.1 We say that an integer a ***divides*** another integer b (denoted by $a \mid b$) if there exists an integer c such that $a \cdot c = b$. In this case, a is called a ***factor*** (or ***divisor***) of b and b is called a ***multiple*** of a. Clearly every natural number other than 1 has at least two factors, 1 and itself. If a number has only these two factors, it is called ***prime***. A natural number with more than two factors is called ***composite***. Notice that 1 is neither prime nor composite. It is called a ***unit***.

The prime numbers are considered the building blocks of all numbers for obvious reasons. All real numbers can be expressed as rational numbers or limits of rational numbers. All rational numbers are ratios of integers. All integers are positive or negative natural numbers. All natural numbers greater than 1 are products of prime numbers. The fact that every natural number greater than 1 is a product of prime numbers (and in fact this representation is unique except for the order) is called the ***Fundamental Theorem of Arithmetic***. Here are few other fundamental principles/theorems that we will need this semester.

Theorem 1.1.2 (Principle of Mathematical Induction - PMI) Let $P(n)$ be a proposition, i.e. a mathematical statement that is either true or false (but not both) for any natural number n. If (a) $P(1)$ is true, and (b) $P(k)$ true implies that $P(k+1)$ is true, then $P(n)$ is true for all n.

This principle is extremely useful for proving something is true for all natural numbers, since a case-by-case study could take a while. The idea is to show that the proposition is true for $n = 1$, and then to show that if it is true for some arbitrary number k, then it must be true for the next number $k+1$. These two facts together show, in domino fashion, that the statement is true for all natural numbers. Since it was true for $n = 1$ it must also be true for $n = 2$. But since it is true for $n = 2$ it must also be true for $n = 3$. But then it must also be true for $n = 4$, and $n = 5$, and so on.

Steps for Mathematical Induction

Let $P(n)$ be a statement. To show $P(n)$ is true for all natural numbers:

1. Show $P(1)$ is true.
2. Assume $P(k)$ is true for an arbitrary $k \in \mathbb{N}$.
3. Show $P(k+1)$ is true.

Example 1.1.3 Prove that $\sum_{i=1}^{n} i = \frac{n(n+1)}{2}$ for all n.

This is a rather famous formula and there is an amusing anecdote involving it. The story revolves around Carl Gauss, the "Prince of Mathematicians." In 1787, at the age of 10, Carl's arithmetic class was apparently giving his teacher fits. The teacher, in an effort to keep the children busy for a few hours, instructed the students to add the numbers from 1 to 100. The precocious Carl scribbled away for a few moments on his slate, and then turned it over and

crossed his arms in satisfaction. The teacher was not amused, but was quite impressed to see what young Carl had done. He had written out the sum to be added two times, once as $1+2+3+\cdots+98+99+100$ and once as $100+99+98+\cdots 3+2+1$. He wrote these two sums one above the other so he could then add numbers in pairs vertically, $1+100$, $2+99$, $3+98$, and so on. Since there were 100 such sums, and they all added to 101, Carl knew that this total sum was $100\cdot 101=10{,}100$. But of course this was twice what the teacher had instructed him to find, so he easily divided by two in order to find the requested sum. Carl Gauss has many wonderful stories about his genius, and is widely considered one of the three greatest mathematicians of all time (along with Archimedes and Sir Isaac Newton). Now, on to the proof.

Proof: For $n=1$ the equation is true since $\sum_{i=1}^{1} i=1$. Now suppose it is true for some natural number k. So $\sum_{i=1}^{k} i=1+2+3+\cdots+(k-1)+k=\frac{k(k+1)}{2}$. We need to show that the equation must then also hold for $k+1$. In other words, we need to show that $\sum_{i=1}^{k+1} i=\frac{(k+1)((k+1)+1)}{2}=\frac{(k+1)(k+2)}{2}$. If we write the sum out as such: $\sum_{i=1}^{k+1} i=1+2+3+\cdots+(k-1)+k+(k+1)$, and group the first k terms, we get $\sum_{i=1}^{k+1} i=\left[1+2+3+\cdots+(k-1)+k\right]+(k+1)$. By assumption, the first k terms can be replaced by $\frac{k(k+1)}{2}$. So we have,

$$\sum_{i=1}^{k+1} i=\left[1+2+3+\cdots+(k-1)+k\right]+(k+1)=\frac{k(k+1)}{2}+(k+1).$$

We can then simplify the expressions on the right side of that equation to get the desired result.

$$\frac{k(k+1)}{2}+(k+1)=\frac{k(k+1)}{2}+\frac{2(k+1)}{2}=\frac{k^2+3k+2}{2}=\frac{(k+1)(k+2)}{2}.$$ ■

If the proposition under consideration is not "for all natural numbers", you should not start at $n=1$. You should always begin with the first relevant case. For example, if the proposition you are proving is for all natural numbers $n\geq 4$, then start with $n=4$. Identifying the initial case seems trivial, and in fact often is, but it is vitally important. Ignoring the initial case or starting with an incorrect number can yield incorrect results.

Example 1.1.4 Prove that for all $n\geq 5$, $n^2<2^n$.

Proof: Clearly $5^2<2^5$, so the proposition is true for $n=5$. Now assume, the

proposition is true for some $k \geq 5$. We need to show that $(k+1)^2 < 2^{(k+1)}$. To do this we'll need to use the fact that $2k+1 < k^2$ for all $k \geq 5$ (in fact it's true for all $k \geq 3$ but we don't need that). This can be shown by looking at the graphs of k^2 and $2k+1$ or by doing some calculus on the function $k^2 - 2k - 1$. Using this fact, we have:

$$(k+1)^2 = k^2 + 2k + 1 < k^2 + k^2 = 2k^2 < 2(2^k) = 2^{k+1}.$$ ■

Exercise 1.1.5 Prove that $n! \leq n^n$ for all natural numbers.

There are several other versions of mathematical induction and in fact several other theorems that can be shown to be equivalent to PMI. The Extended Principle of Mathematical Induction states that if (a) $P(1)$ is true, and (b) $P(n)$ true for all $1 \leq n \leq k$ implies that $P(k+1)$ is true, then $P(n)$ is true for all n. Sometimes assuming $P(n)$ true ***for all*** $1 \leq n \leq k$ is more useful that just assuming $P(k)$ true.

One of the theorems equivalent to PMI is the Well-Ordering Principle. There are many different variations of it, but this is the one that we will use.

Theorem 1.1.6 (Well-Ordering Principle - WOP) Every non-empty set of natural numbers contains a smallest element.

Proof: Let S be a non-empty set of natural numbers. Suppose (by contradiction) that S does not have a least element. Note that $1 \notin S$ since if $1 \in S$, it would be the least element of S and we assumed S did not have a least element. Similarly, if $n \notin S$ for all $1 \leq n \leq k$ (for some natural number k), then $k+1 \notin S$ also since otherwise $k+1$ would be the least element of S. By the Extended PMI, this implies that no natural number is in S, in other words, S is empty. This contradicts our assumption that S is a non-empty set of natural numbers. ■

Theorem 1.1.7 (The Division Algorithm) Let a and b be natural numbers with $a \leq b$. Then there exist two natural numbers q and r (with $0 \leq r < a$) such that $b = aq + r$. The number q is called the ***quotient*** and the number r is called the ***remainder***.

Proof: We will show that q and r exist using the WOP. Define a set S as follows: $S = \{b - ax : x \geq 1 \text{ and } b - ax \geq 0\}$. Since $a \leq b$, $b - a \geq 0$. So $b - a \in S$ and S is non-empty. Therefore, by the WOP, it has a least element, call it r. Since $r \in S$, it follows that $r = b - aq$ for some $q \geq 1$ and $r \geq 0$. So clearly $b = aq + r$. All that is left to show is that $r < a$. If $r \geq a$, then $r - a \geq 0$. Also, $r - a = (b - aq) - a = b - a(q+1)$. So $r - a \in S$. But this contradicts the fact that r was the *least* element of S. So $r < a$. ■