Melbourne High School
Maths Extension Group 2023
Term 2 Week 1 Handout

> *If two numbers by multiplying one another make some number, and any prime number measure the product, it will also measure one of the original numbers.*
>
> —Euclid, *Elements Book VII* (c. 300 BC)

The Fundamental Theorem of Arithmetic

Prime numbers are to the natural numbers what atoms are to matter. They are the fundamental, indivisible building blocks of the universe we call number theory. As such, we might expect there is some grand theorem that explains the importance of primes in higher arithmetic, and in fact there is; this theorem is the Fundamental Theorem of Arithmetic.

Let's begin by considering the number 12. Clearly 12 is composite, because it is divisible by 2. So we write $12 = 2 \times 6$. Turning our attention to 6, we realise it too is composite because it is 2×3. The numbers 2 and 3 being prime, we cannot factorise further, leaving us with $12 = 2 \times 2 \times 3$.. This is called the prime factorisation of 12. What the Fundamental Theorem of Arithmetic asserts is that there is no other way to write 12 as a product of primes other than what we have written down. That is, it is impossible to write down a prime factorisation of 12 without using 2 exactly twice and 3 exactly once and using no other primes. Of course, 12 was just an example; we could've picked any positive integer. But no matter which number we might have picked, the Fundamental Theorem of Arithmetic guarantees that any prime factorisation we work out is unique.

Just to be clear, by 'unique' we mean unique up to reordering of the factors. So we may write $12 = 2 \times 2 \times 3$ or $12 = 2 \times 3 \times 2$, but we have still used 2 twice and 3 once. Also note how this theorem precludes 1 from being a prime, because inserting any number of 1s doesn't change the value of the product.

Mathematicians considered unique factorisation an obvious property of the integers for thousands of years. To illustrate how special this property of the natural numbers is, consider numbers of the form $4k + 1$. These are the numbers beginning

$$1, 5, 9, 13, 17, 21, \ldots .$$

A "prime" in this system is a number that cannot be factorised without going outside of the set of numbers. The first non-prime in this system of numbers is $25 = 5 \times 5$. Just like with the positive integers, each number is either a prime or able to factorised as a product of primes, but this factorisation is not always unique. For example, $693 = 9 \times 77 = 21 \times 33$, and 77, 9, 21, and 13 are all primes in this number system.

Before we examine *unique* factorisation, we first need to verify that every number is actually a product of primes. Fortunately this is easy and follows at once by the definition of prime and composite numbers. The method is by strong induction; try it for yourself.

Note that there is something fishy about 1. This is why we define the empty product to be equal to 1, so that 1 is still a product of primes—it is the product of zero primes.

The real crux of the problem is showing that a prime factorisation is necessarily unique. The most common proof uses Euclid's Lemma, the proof of which we left as an exercise on a previous handout. Here is the proof for completeness.

Euclid's Lemma asserts that if a prime p divides a product ab, then p must divide at least one of a and b. To begin the proof, we assume that p does not divide a, because if it does then we have nothing to prove. Now the aim is to show that p divides b.

If p does not divide a, then $\gcd(p, a)$ must be equal to 1. This follows immediately from p having only itself and 1 as factors by definition. Since $\gcd(p, a) = 1$, there exist positive integers x and y such

that

$$px - ay = 1.$$

(The proof of this was given in the same previous handout on the Euclidean algorithm.)

Multiplying both sides by b, we obtain

$$pbx - aby = b.$$

By hypothesis, p divides ab, so p divides aby. Certainly p divides pbx, so p divides both pbx and aby. Hence p also divides their difference $pbx - aby$, which is b. This completes the proof of the lemma.

We are now able to prove prime factorisation by contradiction. Assume that there exists some positive integer n that has two distinct factorisations: let

$$n = p_1 p_2 \cdots p_r = q_1 q_2 \cdots q_s$$

where all of $p_1, p_2, \ldots, p_r, q_1, q_2, \ldots, q_s$ are primes. Further suppose that this is the smallest number with the property. We can assume this because every subset of the natural numbers has a least element; hence the set of all natural numbers with at least two different prime factorisations also has a least element.

The property of every subset having a least element is called the *well-ordering property* of the natural numbers. It is certainly not true for real numbers. Is there a least element of the set of real numbers in the interval $(0, 1)$?

From our definition of n, we observe that p_1 divides $n = q_1 q_2 \cdots q_s$. By Euclid's lemma p_1 divides either q_1 or $q_2 q_3 \cdots q_s$. If p_1 doesn't divide q_1 then it divides $q_2 q_3 \cdots q_s$. But by reapplication of Euclid's lemma p_1 divides either q_2 or $q_3 q_4 \cdots q_s$. Eventually we find that p_1 divides at least one of the prime factors q_i for some $1 \leq i \leq s$. Assume without loss of generality that this prime is q_1.

Since p_1 and q_1 are both primes, if p_1 divides q_1, then p_1 must equal q_1. This means we can cancel out p_1 and q_1 from both sides of the equation, which yields a smaller number that can be expressed as a product of primes in two different ways. This contradicts our assumption that n is the smallest number with that property, completing the proof.

This proof, although apparently short, is not the most direct method because it relies on the development of the Euclidean algorithm and the properties of numbers and their greatest common divisors. Gauss offered a shorter proof using modular arithmetic, and there is an even more direct proof that does not require any preliminary lemmas. Both are left as exercises.

The property of prime factorisation seems neat, but why is it useful? There are many reasons why the theorem deserves its grand name; the main one is that it allows us to develop theorems about all the natural numbers by first focusing on the primes. If we can answer some question about the primes, it is likely we can answer the same question about all positive integers. Consider the following example.

We define a function $\sigma(n)$ to be the sum of the divisors of n. For example, $\sigma(6) = 1 + 2 + 3 + 6 = 12$. Suppose our goal is to find a formula for $\sigma(n)$. By computing the first twenty or so values, we observe that the formula is unlikely to be a nice algebraic function, since $\sigma(n)$ doesn't seem to be increasing, decreasing, or exhibiting any sort of behaviour we might expect from a polynomial or exponential function. The way to get started is by looking first at the case when n is prime.

I chose 6 because it's an example of a *perfect number*, which is a number that is equal to the sum of its divisors except itself. This means a number n is perfect if $\sigma(n) = 2n$.

What is $\sigma(p)$ for any prime p? This is easy because the only divisors of p are itself and 1, so $\sigma(p) = p + 1$. The next step up is to consider powers of p. What is $\sigma(p^k)$ for any nonnegative integer k? Here is our first use of the fundamental theorem. Since the factorisation p^k is unique, no other prime can divide it. Hence the only divisors are the

powers of p, namely $1, p, p^2, \ldots, p^k$. Summing these together yields

$$\sigma(p^k) = 1 + p + p^2 + \cdots + p^k.$$

This sum is just a geometric series with first term 1 and common ratio p; therefore it has the following nice formula:

$$\sigma(p^k) = \frac{p^{k+1} - 1}{p - 1}.$$

We have succeeded in the first part of our plan. Having found a formula for $\sigma(p^k)$ we can find a general formula for $\sigma(n)$. This is left as an exercise.

This idea of first examining a problem for primes and then generalising to all natural numbers is a common theme in number theory. Another example is the classical problem about which numbers are the sum of two squares, which we shall examine in the future. Fermat conjectured, and Euler proved, that every prime of the form $4k + 1$ is the sum of two squares. Using this result and a multiplicative property of such numbers, Euler was able to determine a general criterion for which numbers can be expressed as the sum of two squares.

Problems

1. In this problem we complete out investigation of perfect numbers.

   (a) The divisors of 5 are 1 and 5, and the divisors of 4 are 1, 2, and 4. Note that the divisors of their product, 20, are 1, 2, 4, 5, 10, and 20. By considering further examples if necessary, show that if m and n are coprime then

   $$\sigma(mn) = \sigma(m)\sigma(n).$$

   (b) By the Fundamental Theorem of Arithmetic, every positive integer can be written as

   $$n = p_1^{a_1} p_2^{a_2} p_3^{a_3} \cdots p_r^{a_r}$$

   where all of $p_1, p_2, \ldots, p_r$ are distinct primes. Find a general formula for $\sigma(n)$.

2. (a) From our present view, knowing the Fundamental Theorem, it is obvious that if two numbers are both less than a prime p, then their product is not divisible by p, because p cannot possibly occur in the factorisation of either of the two numbers. Prove this without relying on unique factorisation.

   (b) Hence show that if $a \not\equiv 0 \pmod{p}$ and $b \not\equiv 0 \pmod{p}$ then $ab \not\equiv 0 \pmod{p}$.

   This is equivalent to Euclid's lemma (it's the contrapositive). Therefore by completing this question you have also proved the Fundamental Theorem of Arithmetic in a different way.

3. (a) Suppose that a number n has two different prime factorisations and it is the smallest number with the property. This means all of $1, 2, \ldots, n-1$ can be uniquely factorised. Let

   $$n = p_1 p_2 \cdots p_r = q_1 q_2 \cdots q_s$$

   where all of $p_1, p_2, \ldots, p_r, q_1, q_2, \ldots, q_s$ are primes. Note that none of the p's equal any of the q's, because otherwise they could be cancelled to yield a smaller number with two different factorisation, which contradicts our definition of n. Show that there exist numbers i and j such that $n - p_i q_j > 0$.

   (b) Let $N = n - p_1 q_1$. Clearly, N is less than n, and so can be factorised in only one way by hypothesis. Show that the product $p_1 q_1$ must divide n.

   (c) Hence complete the proof of the Fundamental Theorem of Arithmetic.