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

§1. From Euclid to Gauss

The Fundamental Theorem of Arithmetic states a seemingly obvious, but certainly not trivial, fact about the positive integers. It asserts that every positive integer can be uniquely expressed as a product of prime numbers; that is, there is only way to break a number down into primes. (Of course, we consider rearranging the prime factors to be the same factorisation.) For example, the number 12 is $2 \times 2 \times 3$; it is impossible to write down a factorisation of 12 without using 2 exactly twice and 3 exactly once.

The idea that unique factorisation is an obvious property of the integers was taken for granted for thousands of years. Furthermore, mathematicians assumed that prime factorisation holds for other number systems, which is simply not true. For example, consider numbers of the form $4k + 1$; these are the numbers beginning

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

A "prime" in this system of numbers is a number that is not able to factorised without going outside of the set of numbers. The first non-prime in this system of numbers is 25. 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.

If prime factorisation were a general theorem for virtually all number systems, Fermat's Last Theorem would have been successful proven in the 19th century. The really first rigorous proof of the fundamental theorem was given by Gauss in the early 19th century and used modular arithmetic. Here we shall consider several common proofs of the theorem.

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.

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. For completeness, here is the proof of the lemma.

Recall that Euclid's Lemma asserts that if a prime p divides a product ab, then p must divide at least one of a and b. That is, p either divides a, b, or both. To begin the proof, we assume that p does not divide a, because if it did, 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, by definition, only itself and 1 as factors. 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

$$pbx - aby = b.$$

We have found an expression for 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.

Using this lemma, we are 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 it is a proerty of the natural numbers that every subset has a least element; hence the set of all natural numbers with at least two different prime factorisations also has a least element.

From our definition of n, we see 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 will find that p_1 divides at least one of the prime factors q_i. 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.