MAT246H1S Lec0101 Burbulla

Chapter 4 Lecture Notes
The Fundamental Theorem of Arithmetic

Winter 2019

Chapter 4: The Fundamental Theorem of Arithmetic

4.1: Proof of The Fundamental Theorem of Arithmetic

What is the Fundamental Theorem of Arithmetic?

As we saw in Chapter 2, Theorem 2.2.4 stated that every natural number other than 1 is a product of prime numbers. So for example

1. $144 = 2 \cdot 2 \cdot 2 \cdot 2 \cdot 3 \cdot 3 = 2^4 \cdot 3^2$.
2. $3,978 = 2 \cdot 3 \cdot 3 \cdot 13 \cdot 17 = 2 \cdot 3^2 \cdot 13 \cdot 17$
3. $40,041 = 3 \cdot 3 \cdot 3 \cdot 1483 = 3^3 \cdot 1483$

Of course, finding the factors may not be easy. However, one thing we can establish is that for every natural number its prime factors are uniquely determined. That is, the *only* prime factors of 144 are 2 and 3; the *only* prime factors of $3,978$ are $2, 3, 13$ and 17; the *only* prime factors of $40,041$ are 3 and $1,483$. This fact is known as the Fundamental Theorem of Arithmetic, and we shall prove it by contradiction.

The Fundamental Theorem of Arithmetic

Theorem 4.1.1: Every natural number greater than 1 can be written as a product of primes, and the expression of a number as a product of primes is unique except for the order of the factors.

Comment: the first statement is just Theorem 2.2.4. What remains to show is that the expression of a number as a product of primes is *unique,* except for the order of primes. There are at least two approaches in mathematics to show that something is unique:

1. suppose that you have two of them, and then show they must equal each other; or
2. suppose that you have two of them, and then derive a contradiction.

We will use the second approach.

Proof of the Fundamental Theorem of Arithmetic

Proof: by contradiction. Let T be the set of numbers that have at least two different representations as a product of primes. Suppose $T \neq \emptyset$. By the well-ordering principle there is a least number in T, call it N, that has at least two different representations as a product of primes. That is, there are primes $p_1, p_2, \ldots, p_r$ and other primes $q_1, q_2, \ldots, q_s$, such that

$$N = p_1 \cdot p_2 \cdots p_r = q_1 \cdot q_2 \cdots q_s.$$

Neither r nor s can be 1: if $r = s = 1$, then $N = p_1 = q_1$ and the two representations are the same; and if $r = 1$ and $s > 1$, then $N = p_1 = q_1 \cdot q_2 \cdots q_s$, contradicting the fact that p_1 is prime. In fact $\{p_1, p_2, \ldots, p_r\} \cap \{q_1, q_2, \ldots, q_s\} = \emptyset$, for if $p_i = q_j = p$, then $N/p < N$ and N/p would also be in T, contradicting the fact that N is the least element in T. In particular, we know $p_1 \neq q_1$. One of these two primes must be less than the other; assume $p_1 < q_1$.

Let $M = N - p_1 \cdot q_2 \cdot q_3 \cdot \cdots \cdot q_s < N$. Substituting for N as a product of the p_i primes we have

$$M = p_1 \cdot p_2 \cdots p_r - p_1 \cdot q_2 \cdot q_3 \cdots q_s = p_1(p_2 \cdots p_r - q_2 \cdot q_3 \cdots q_s),$$

implying that p_1 divides M. (In particular, $M > 1$.) Since $M < N$, M has a unique factorization into primes. Now substitute for N as a product of the q_j primes to obtain

$$M = q_1 \cdot q_2 \cdots q_s - p_1 \cdot q_2 \cdot q_3 \cdots q_s = (q_1 - p_1) \cdot q_2 \cdots q_s,$$

and the unique factorization of M into primes must be the unique factorization of $q_1 - p_1$ into primes, times $q_2, q_3, \ldots, q_s$. Since p_1 divides M and $p_1 \neq q_j$, we know that p_1 divides $q_1 - p_1$. So there is a number n such that

$$q_1 - p_1 = p_1 \cdot n \Leftrightarrow q_1 = p_1 + p_1 \cdot n \Leftrightarrow q_1 = p_1(1 + n).$$

This implies that p_1 divides q_1, which contradicts the fact that they are distinct primes. Thus $T = \emptyset$. $\square$

Two Corollaries of the Fundamental Theorem of Arithmetic

Corollary 4.1.2: every natural number n greater than 1 has a canonical factorization into primes: that is

$$n = p_1^{\alpha_1} \cdot p_2^{\alpha_2} \cdots p_r^{\alpha_r},$$

where each p_i is a prime, $p_i < p_{i+1}$, and α_i is a natural number.

Example: $60,368 = 2^4 \cdot 7^3 \cdot 11$. Also, see the examples at the beginning of this section.

Corollary 4.1.3: if p is a prime and a and b are natural numbers such that p divides $a \cdot b$, then p divides a or p divides b.

Example: $7 \mid 294 = 6 \cdot 49$ so $7 \mid 6$ or $7 \mid 49$. Which is it? $7 \mid 49$.

Warning: $18 \mid 270 = 30 \cdot 9$ but 18 divides neither 30 nor 9.

Proof of Corollary 4.1.3

Since $p \mid ab$ there is natural number d such that $ab = pd$. So the unique factorization of ab into a product of primes includes the prime p. On the other hand, there are primes p_i and q_j such that

$$a = p_1^{\alpha_1} \cdot p_2^{\alpha_2} \cdots p_r^{\alpha_r} \text{ and } b = q_1^{\beta_1} \cdot q_2^{\beta_2} \cdots q_s^{\beta_s},$$

which means

$$a\,b = p_1^{\alpha_1} \cdot p_2^{\alpha_2} \cdots p_r^{\alpha_r} \cdot q_1^{\beta_1} \cdot q_2^{\beta_2} \cdots q_s^{\beta_s}.$$

Thus the prime p must be present in the factors on the right hand side:

1. p could be p_i, for some i, in which case $p \mid a$; or
2. p could be q_j, for some j, in which case $p \mid b$; or
3. p could be both p_i for some i and q_j for some j, in which case $p \mid a$ and $p \mid b$.