The Fundamental Theorem of Arithmetic

Reading

- Section 6.1

Practice Problems

6.1 1, 2, 3, 4, 5, 6, 8, 11, 16, 17
Challenge 6.1 (Optional) 9, 10, 21, 22, 23, 24

Notes

The **Fundamental Theorem of Arithmetic** is straightforward:

> Every natural number $n > 1$ can be written as a product of prime numbers, and this factorization is unique up to reordering of the factors.
>
> In particular, if we collect same prime factors together in one term, and order according to size, we get a unique expression of the form:
>
> $$n = p_1^{k_1} p_2^{k_2} p_3^{k_3} \cdots p_s^{k_s}$$
>
> where $p_1 < p_2 < \cdots < p_s$ are prime, and all $k_i > 0$.

We have already proven such an expression exists. We now have to prove uniqueness. This will follow from a key property of prime numbers:

> If p is prime and $p|ab$, then it must be the case that $p|a$ or $p|b$.
>
> In other words, a prime cannot divide a product without dividing one of the factors.
>
> This extends naturally to more than 2 terms.

We now prove this fact. This in fact follows from our work with Euclidean division and the gcd.

- We assume that $p|ab$.
- If $p|a$ we are done. Therefore we assume p does not divide a, and we want to show that $p|b$.
- Since p is prime and does not divide a, we saw previously that it must be the case that $\gcd(p, a) = 1$.
- We also saw earlier that if a number divides a product and is relatively prime to the first term, then it must fully divide the second term. (Euclid's lemma)

- Therefore $p|b$.

  Aside:

  In other number systems where Euclidean Division doesn't hold, there are two different types of elements:

  - Those elements that satisfy "If $p|ab$ then $p|a$ or $p|b$" are called *prime elements*.
  - Those elements that satisfy "If $p = ab$ then either a or b equals ± 1" are called *irreducible elements*.

  Every prime element is irreducible, but the converse is not always true. If You have Euclidean Division, the above proof shows that it is true.

Now we proceed to *prove the Fundamental Theorem*.

- Suppose we can write n as a product of primes in possibly two different ways:

$$n = p_1 p_2 p_3 \cdots p_k$$

$$n = q_1 q_2 q_3 \cdots q_m$$

  possibly involving different prime numbers and a different number of numbers.

- Since p_1 divides $n = q_1 q_2 q_3 \cdots q_m$, it must divide one of the q_i.
- Up to reordering of the q_i's we can assume that p_1 divides q_1.
- But a prime number cannot divide another prime number unless they are equal.
- So $p_1 = q_1$.
- Cancelling out those common terms, we get:

$$p_2 p_3 \cdots p_k = q_2 q_3 \cdots q_m$$

- We can now repeat the same procedure to get that, up to reordering, $p_2 = q_2$, $p_3 = q_3$ etc.
- If one of the sequences ends before the other, we end up with an equation saying that 1 is equal to a product of one or more primes, which is impossible.
- So there must be the same number of factors, and they must equal each other up to a reordering.