Section 1.3: Prime and composite numbers

Definition 1.12 Let n be a natural number with $n > 1$. We say that n is prime if the only positive divisors of n are 1 and n. If n is not prime, then we call it composite.

Theorem 1.13 The Fundamental Theorem of Arithmetic [FTA] Let n be a natural number with $n > 1$. Then there are primes $p_1 < p_2 < \ldots < p_r$ and naturals $k_1, k_2, \ldots, k_r$ with

$$n = {p_1}^{k_1} {p_2}^{k_2} \ldots {p_r}^{k_r}.$$

Further, the primes, p_i, and the naturals, k_i, are unique.

NB. We often paraphrase the FTA by saying that every natural number greater than one can be 'uniquely' decomposed into the product of prime factors. Here 'uniquely' means 'uniquely up to the order in which the factors are listed.'

Theorem 1.14 [Euclid] There are infinitely many primes.

Lemma Let a, b, q_1, and q_2 be integers with $a = 4q_1 + 1$ and $b = 4q_2 + 1$. Then there is an integer q for which $ab = 4q + 1$.

NB. This lemma says that if two numbers have a remainder of 1 upon division by 4, then their product will leave a remainder of 1 upon division by 4. [You should start to make a habit of paraphrasing propositions in 'plain English;' it should help you to fit ideas together.]

Proposition 1.15 There are infinitely many primes of the form $4q + 3$.