

Supplement to Ch. 7:
Alternate forms of the Fundamental Theorem of Arithmetic
Math 126, Fall 2009

Some odds and ends about the FTA:

Why 1 is not prime. Note that if 1 were a prime, then prime factorization would *not* be unique, as would could find a “different” factorization of any number by adding some 1’s:

$$n = p_1 p_2 \dots p_r = (1)p_1 p_2 \dots p_r = (1)(1)p_1 p_2 \dots p_r = \dots \quad (1)$$

and so on.

Fundamental Theorem of Arithmetic, with the primes grouped. By grouping repeated primes in the factorization of a number, we can express the FTA in the following way:

Theorem (Fundamental Theorem of Arithmetic). *Let n be an integer ≥ 2 . Then n can be uniquely expressed in the form*

$$n = p_1^{a_1} p_2^{a_2} \dots p_r^{a_r}, \quad (2)$$

where the p_i are prime, the a_i are positive integers, and $p_1 < p_2 < \dots < p_r$.

Note that assuming that the primes are written in increasing order removes the question of reordering.

When we want to compare the prime factorizations of two different numbers m and n , it is sometimes useful to write

$$m = p_1^{a_1} p_2^{a_2} \dots p_r^{a_r}, \quad n = p_1^{b_1} p_2^{b_2} \dots p_r^{b_r}, \quad (3)$$

where the p_i are prime, $p_1 < p_2 < \dots < p_r$, and the a_i and b_i are *nonnegative* numbers (i.e., we allow some $a_i = 0$ and $b_i = 0$). We allow 0th powers of primes in the factorizations of m and n , which are then no longer unique, because we may then assume that the same primes p_1, \dots, p_r appear in both factorizations.

Using the grouped version of FTA. Suppose m and n are integers ≥ 2 that are factorized as in (3). It is interesting to try to understand some of the concepts from Chs. 1–6 using these prime factorizations. Specifically:

1. Under what conditions on the a_i and b_i does m divide n ? Try some examples and find a pattern; see if you can prove your pattern.
2. We say that n is *square-free* if the only integer d such that d^2 divides n is $d = 1$. Under what conditions on the a_i is m square-free? Try some examples and find a pattern; see if you can prove your pattern.
3. Find a formula for $\gcd(m, n)$ in terms of the a_i and b_i . Prove that your formula works.
4. Find a formula for $\text{lcm}(m, n)$ in terms of the a_i and b_i . Prove that your formula works.