

Fundamental Theorem of Arithmetic

**Collaborators:**

Here we restrict our attention to the integers. Given integers  $a$  and  $b$ , we say “ $a$  divides  $b$ ” or “ $b$  is divisible by  $a$ ”, and we write  $a \mid b$ , if there exists another integer  $c$  such that  $ac = b$ . An integer  $p$  is called **prime** if  $a \mid p$  implies  $a = \pm 1$  or  $a = \pm p$ . Since negative numbers do not significantly add anything interesting to the theory of divisibility, we typically restrict our attention further to nonnegative integers.

<p><b>HW: Liebeck Chapter 10, Problem 4(b)</b> Suppose <math>a, b</math> are integers such that <math>a \mid b</math> and <math>b \mid a</math>. Prove that <math>a = \pm b</math>.</p>
---

**Theorem** (Fundamental Theorem of Arithmetic). *Let  $n \geq 2$  be an integer.*

(a) *Then  $n$  is equal to a product of prime numbers,*

$$n = p_1 \cdots p_k,$$

*where  $p_1, \dots, p_k$  are prime and  $p_1 \leq p_2 \leq \cdots \leq p_k$ .*

(b) *This **prime factorization** is unique. That is, if*

$$n = p_1 \cdots p_k = q_1 \cdots q_\ell$$

*with  $p_i, q_i$  prime as in part (a), then  $k = \ell$  and  $p_i = q_i$  for all  $i$ .*

Let  $n = p_1^{a_1} \cdots p_k^{a_k}$ , where the  $p_i$  are prime with  $p_1 < \cdots < p_k$  and the  $a_i$  are positive integers. Show that if  $m \mid n$ , then

$$m = p_1^{b_1} \cdots p_k^{b_k}$$

with  $0 \leq b_i \leq a_i$  for all  $i$ .