

## Primes and Factorization

**Definition 1** (Prime). We say an integer  $p \notin \{1, 0, -1\}$  is prime if whenever  $p = ab$ , either  $a = \pm p$  or  $b = \pm p$ . Equivalently,  $p$  is prime if it is not 0, 1, or -1, and the only divisors of  $p$  are  $\pm 1$  and  $\pm p$ .

**Proposition 1.**

1. 2 and 3 are prime.
2. If  $p$  is prime, then  $-p$  is prime.
3. If  $p$  and  $q$  are prime such that  $p|q$ , then  $q = \pm p$ .
4. If  $p$  is a prime integer, then for all integers  $a$ ,  $\gcd(a, p)$  is  $|p|$  if  $p|a$  and 1 otherwise.

**Proposition 2.** An integer  $p$  is prime if and only if whenever  $p|ab$ , either  $p|a$  or  $p|b$ .

*Proof.* This is an “if and only if” statement; we proceed by proving the “only if” part and then the “if” part.

( $\Rightarrow$ ) Suppose  $p$  is prime and that  $p|ab$ . Consider  $\gcd(a, p)$ . Since  $p$  is prime, there are two possibilities.

- If  $\gcd(a, p) = |p|$ , then  $|p|$  divides  $a$ , so that  $p|a$ .
- If  $\gcd(a, p) = 1$ , then by Euclid’s Lemma,  $p|b$ .

( $\Leftarrow$ ) Suppose  $p$  has the property that if  $p|ab$  then either  $p|a$  or  $p|b$ . Suppose further that  $p = ab$ . In particular  $p|ab$  (since  $1 \cdot p = ab$ ) and so, without loss of generality,  $p|a$ . Say  $a = pa'$ . Now  $p = ab = pa'b$ , and thus  $1 = a'b$ . Now  $|b| = 1$ , and thus  $|p| = |a|$ , so that  $p = \pm a$  as needed.  $\square$

**Corollary 3.** If  $p$  is a prime and  $a_i$  integers such that  $p|a_1a_2 \cdots p_n$ , then  $p|a_i$  for some  $i$ .

## Prime Factorization

**Theorem 4** (Fundamental Theorem of Arithmetic: Part 1). Every integer other than 0, 1, and  $-1$  can be written as a product of primes. That is, every such  $n$  can be expressed as  $n = p_1p_2 \cdots p_k$ , where the  $p_i$  are prime. This is called a prime factorization of  $n$ .

*Proof.* Suppose first that  $b > 0$ . We proceed by strong induction.

- **Base Case** ( $b = 2$ ): If  $d|2$ , then  $0 < |d| \leq |2|$ . Thus the only possible divisors of 2 are  $\pm 1$  and  $\pm 2$ , and so 2 is prime by definition.

- **Inductive Step:** Suppose that for some  $n$ , every integer  $2 \leq n' < n$  can be written as a product of primes, and consider  $n$ . If  $n$  is itself prime, then  $n = n$  is its own prime factorization. If  $n$  is not prime, then there exist integers  $a$  and  $b$  such that  $n = ab$  and  $n \neq \pm a$  and  $n \neq \pm b$ . Since  $n > 0$ , we can assume that  $a > 0$  and  $b > 0$ . In fact we have  $a > 1$  and  $b > 1$ , so that  $a, b < n$ . By the inductive hypothesis,  $a$  and  $b$  have prime factorizations; say  $a = p_1 p_2 \cdots p_h$  and  $b = q_1 q_2 \cdots q_k$ . Now

$$n = ab = p_1 p_2 \cdots p_h q_1 q_2 \cdots q_k$$

has a prime factorization.

Thus by strong induction every integer  $n \geq 2$  has a prime factorization. If  $n < 0$ , then  $-n > 0$ , so that  $-n = p_1 p_2 \cdots p_k$  has a prime factorization; then  $n = (-p_1) p_2 \cdots p_k$  also has a prime factorization.  $\square$

**Theorem 5** (Fundamental Theorem of Arithmetic: Part 2). *The prime factorization of an integer is unique in the following sense. If  $n$  has two prime factorizations*

$$n = p_1 p_2 \cdots p_k = q_1 q_2 \cdots q_\ell,$$

*then  $k = \ell$  and, after relabeling the  $q_i$ , we have  $p_i = \pm q_i$  for each  $1 \leq i \leq k$ .*

*Proof.* We saw in FTA Part 1 that every such  $n$  has at least one prime factorization, which consists of at least one prime factor. We will proceed by strong induction on the *length* of the shortest prime factorization of  $n$ .

1. **Base Case:** Suppose  $n = p$  has a prime factorization of length 1; that is,  $n$  itself is prime. Suppose  $p = q_1 q_2 \cdots q_\ell$  is another prime factorization of  $n$ . Since  $p$  is prime, we have (rearranging the  $q_i$  if necessary)  $p | q_1$ . Since  $p$  and  $q_1$  are prime, we have  $q_1 = \pm p$ . Now if  $\ell > 1$  we have

$$1 = |q_2 \cdots q_\ell|,$$

so that  $|q_i| = 1$  for each  $q_i$ , a contradiction. So in fact  $\ell = 1$  and  $q_1 = \pm p$ , as claimed.

2. **Inductive Step:** Suppose that every integer having a shortest prime factorization of length at most  $k$  has a unique prime factorization, and suppose  $n = p_1 p_2 \cdots p_{k+1}$  is an integer with a shortest prime factorization of length  $k + 1$ . Suppose further that  $n = q_1 q_2 \cdots q_\ell$  is another prime factorization of  $n$ . In particular,  $p_1 | q_1 q_2 \cdots q_\ell$ , so that, rearranging the  $q_i$  if necessary,  $p | q_1$ . Now  $q_1 = \pm p$ , and we have

$$p_2 \cdots p_{k+1} = q_2 \cdots q_\ell.$$

Note that these are two prime factorizations of an integer having a shortest prime factorization of length at most  $k$ . By the Inductive Hypothesis, we have  $\ell = k + 1$  and, relabeling the  $q_i$  if necessary,  $q_i = \pm p_i$  for each  $2 \leq i \leq k + 1$ . So the prime factorization of  $n$  is unique.  $\square$

## Proving Primality

**How do we prove that a given integer is prime?** The definition suggests one way to do it, known as *trial division*: an integer  $n$  is prime if and only if  $n$  is not divisible by any integer  $t$  with  $1 < t < n$ . This works, but is extremely time consuming. A better method is suggested by the following.

**Proposition 6.** *Let  $n > 1$  be an integer, and let  $t$  be the largest integer such that  $t^2 < n$ . (Such an integer exists, since the set of all  $t$  with  $t^2 < n$  is bounded above by  $n$ .) (Also, this  $t$  is  $\lfloor \sqrt{n} \rfloor$ , but we don't know what  $\sqrt{\cdot}$  means.) Then  $n$  is prime if and only if  $n$  is not divisible by any prime  $p$  with  $2 \leq p \leq t$ .*

*Proof.* Certainly if  $n$  is prime it is not divisible by any such  $p$ . We prove the “only if” part by contraposition. Suppose that  $n$  is *not* prime; say  $n = ab$ , where  $n \neq a$  and  $n \neq b$ . (We can assume positive signs here since  $n > 0$ .) If  $a$  and  $b$  are both strictly larger than  $t$ , then we have  $n > t^2 > ab > n$ , a contradiction. Without loss of generality, then,  $a \leq t$ . In particular, all prime factors of  $a$  are less than  $t$  in absolute value, and so  $n$  has a prime factor  $p$  such that  $2 \leq p \leq t$ .  $\square$

For example, consider  $n = 5$ . The largest  $t$  such that  $t^2 < 5$  is  $t = 2$ , and the only prime  $p$  such that  $2 \leq p \leq 2$  is  $p = 2$ . Since (by the Division Algorithm) we have  $5 = 2 \cdot 2 + 1$ , with remainder  $1 \neq 0$ , 2 does not divide 5. So **5 is prime**.

This result gives us a strategy for finding prime numbers, but it only works if we have a complete list of primes up to  $\sqrt{n}$  to begin with. In other words, we can find a prime if we start with a list of primes. This can be made into a reasonably efficient algorithm for finding all the primes up to some bound, called the *Sieve of Eratosthenes*. There are some interesting questions left unanswered, though. Given an integer  $n$ ,

- ...is  $n$  prime?
- ...what is the prime factorization of  $n$ ?
- ...how many prime factors does  $n$  have?
- ...how many *distinct* prime factors does  $n$  have?
- ...what is the smallest prime factor of  $n$ ?
- ...how difficult is it to answer these questions?
- ...how difficult is it to *verify* the answers to these questions?