

**READING TO ACCOMPANY CSU-P MATH 319
NUMBER THEORY
SPRING TERM, 2014**

JONATHAN A. PORITZ *AFTER* WISSAM RAJI

3. PRIMES AND THE FUNDAMENTAL THEOREM OF ARITHMETIC

Primes are the atoms out of which the more complicated, composite integers (the molecules, in this metaphor) are built. In this section we study some of their basic properties and then prove the aptly named Fundamental Theorem of Arithmetic.

First of all, we make the

Definition 3.1. We say $p \in \mathbb{N}$ is **prime** if $p > 1$ and the only natural numbers which divide p are 1 and p .

Example 3.2. Some primes are 2, 3, 5, 7, 11, 13, and 17. Notice 2 is the only even prime (clearly – any other would be a multiple of 2 and hence could not be prime), and has some unusual properties – the joke is that “2 is the oddest prime.”

The largest prime known to humans at the time of this writing is

$$2^{57,885,161} - 1$$

which was proven to be prime in January of 2013 by a distributed computer program called **GIMPS** [the “Great Internet Mersenne Prime Search”] running on hundreds of machines across the Internet.

In contrast, we also use the following term

Date: 24 February 2014 00:30 These notes are adapted by Jonathan Poritz from **An Introductory Course in Elementary Number Theory** by Wissam Raji, see www.saylor.org/books/. Both these notes and Raji’s text are released under a Creative Commons **CC BY 3.0** license, see

<https://creativecommons.org/licenses/by/3.0/>



Definition 3.3. A number $c \in \mathbb{N}$ which is greater than 1 and not prime is called **composite**.

How far does a naive, brute-force check have to go in order to see if a number is composite?

Theorem 3.4. *If n is a composite, then it has a positive divisor d satisfying $d \leq \sqrt{n}$.*

Proof. Suppose n is composite. Then it has some divisor $a \in \mathbb{N}$. Notice that $n = a \cdot \frac{n}{a}$, so $\frac{n}{a} \in \mathbb{N}$ is also a divisor. But a and $\frac{n}{a}$ cannot both be less than $\sqrt{n}$, because if they were we would have

$$n = a \cdot \frac{n}{a} < \sqrt{n} \cdot \sqrt{n} = n$$

which would be a contradiction. Hence either a or $\frac{n}{a}$ is the divisor d promised by the theorem statement. $\square$

Euclid's Lemma (Lemma 2.6) takes a particularly nice form if the divisor involved is prime:

Proposition 3.5. *Suppose p is a prime and $a, b \in \mathbb{Z}$. If $p \mid ab$ then $p \mid a$ or $p \mid b$.*

Proof. Notice that $\gcd(p, a) \mid p$, therefore $\gcd(p, a)$ is either 1 or p since p is prime. But also $\gcd(a, p) \mid a$, so either $p \mid a$ or $\gcd(a, p) = 1$. If $p \mid a$, we are done. If not, since therefore $\gcd(a, p) = 1$, Euclid's Lemma tells us that $p \mid b$. $\square$

A more general form of this is

Corollary 3.6. *Suppose p is a prime, $k \in \mathbb{N}$, and $a_1, \dots, a_k \in \mathbb{Z}$. Then if $p \mid a_1 \dots a_k$, it follows that p divides at least one of the a_j .*

Proof. Left to the reader (use induction on k). $\square$

This leads to the aptly named

The Fundamental Theorem of Arithmetic. Let $n \in \mathbb{N}$. Then $\exists k \in \mathbb{N}$ and primes $p_1, \dots, p_k$ such that $n = p_1 \dots p_k$. Furthermore, if $l \in \mathbb{N}$ and $q_1, \dots, q_l$ are also primes such that $n = q_1 \dots q_l$, then $l = k$ and the factorization in terms of the q 's is merely a reordering of that in terms of the p 's.

Proof. We use the Second Principle of Mathematical induction for the existence part. The general statement we are proving is $\forall n \in \mathbb{Z}, n > 1 \Rightarrow S(n)$, where $S(n)$ is the statement “ $\exists k \in \mathbb{N}$ and primes $p_1, \dots, p_k$ such that $n = p_1 \dots p_k$.”

As the base case, say $n = 2$. Then $k = 1$ and $p_1 = 2$ works.

Now assume $S(k)$ is true for all $k < n$. If n is prime, then $k = 1$ and $p_1 = n$ works. So suppose n is instead composite, with divisor $d \neq 1, n$. Then both $d, \frac{n}{d} < n$, so by the inductive hypothesis $\exists k, k' \in \mathbb{N}$ and primes $p_1, \dots, p_k, p'_1, \dots, p'_{k'}$ such that $d = p_1 \dots p_k$ and $\frac{n}{d} = p'_1 \dots p'_{k'}$. So then n is the product

$$n = p_1 \dots p_k \cdot p'_1 \dots p'_{k'}$$

of the $k + k'$ primes. Hence $S(n)$ is true as well, and so prime factorizations always exist.

Now suppose $n \in \mathbb{Z}$ satisfies $n > 1$ and $\exists k, l \in \mathbb{N}$ and both primes $p_1, \dots, p_k$ and $q_1, \dots, q_l$ such that

$$p_1 \dots p_k = n = q_1 \dots q_l.$$

Certainly p_1 divides the left hand side of these dual expressions for n . Then by Corollary 3.6, p_1 divides one of the q_j , which means it must be that $p_1 = q_j$ since they are prime. Removing the p_1 from the left and the q_j from the right, we get

$$p_2 \dots p_k = n = q_1 \dots q_{j-1} \cdot q_{j+1} \dots q_l.$$

Continuing in this way, either we get the uniqueness statement in the theorem, or we run out of p 's or q 's. However, we cannot run out of primes on one side before the other, because that would make a product of primes on one side equal to 1, which is impossible. $\square$

Exercises

- (1) Provide all the details of the proof of Corollary 3.6.
- (2) State and prove a theorem about the prime factorizations of numbers $a, b \in \mathbb{N}$ and of their gcd.
- (3) A number $n \in \mathbb{Z}$, $n > 1$ is called *square-free* if it is not divisible by the square of any natural number other than 1. Prove that an $n \in \mathbb{Z}$, $n \geq 1$ is square-free if and only if it is the product of distinct primes.