Prime Numbers (Theorems and the Infinitude of Primes)

D A V I D  A N D R E W  S M I T H

dave4math.com

Keywords: prime numbers, Sieve of Eratosthenes, prime divisors, Infinitude of Primes, divisor, composites, prime factor theorem

Abstract: We discuss the difference between composites and prime numbers and then show how to find prime numbers using Eratosthenes’ sieve. We then prove the infinitude of prime numbers and show that every natural number has a prime divisor by assuming the well-ordering axiom.

Contents

1 Prime Number Theorems Today ........................................... 2
2 Primes and Composites .................................................... 2
3 Working with Primes ....................................................... 3
4 Sieve of Eratosthenes ..................................................... 3
5 Prime Divisors ............................................................ 4
6 Infinitude of Primes ....................................................... 5
7 Exercises ................................................................. 6
References ................................................................. 7

The mathematical properties of prime numbers began to draw the interests of mathematicians from as early as Ancient Greece. Most of these ancient mathematicians attempted to find the largest prime number that can exist. However, it was until circa 300 BC that Euclid proved that no such thing as the largest prime number can possibly exist.

Yet still, subsequent mathematicians dedicated their time to trying to find a formula by which one could establish an unending series of prime numbers. It is through this quest that the prime number theorem emerged.

†These notes correspond to the following video on the Dave4Math YouTube Channel: https://www.youtube.com/watch?v=Am2I2EMBPAM
1 Prime Number Theorems Today

Today, these theorems have extensive application in number theory, in which they not only give us the fundamental theory of arithmetic that is a cornerstone of the mathematics of integers, but also helps explain how the prime numbers are distributed asymptotically among the integers.

Among the facts that have come to be classified under the umbrella of prime number theorem includes the infinite nature of primes, the ability to factorize every positive integer into a product of primes, Euler’s Theorem on reciprocals of prime numbers, Mersenne primes, Fermat’s primes, among others.

One fundamental method that has proven quite efficient in the process of establishing prime numbers is the sieve of Eratosthenes, although its efficiency is limited to finding prime numbers that lie between one and ten million.

2 Primes and Composites

Several of the most basic and interesting questions concerning the integers involves the prime numbers. For example, are there infinitely many primes of the form \( n^2 + 1 \)? This question is easy to understand, but no one has been able to answer it.

From a certain point of very, the prime numbers are the building blocks for the integers; that is to say, every integer greater than 1 has a prime factor. Indeed, every positive integer is a product of primes. This result was known to the ancient Greeks and is sometimes referred to as Euclid’s lemma.

One of the first questions that comes to mind is concerning prime numbers is:

- how many prime numbers are there?
- why are primes so important to talk about?
- without using trial division, how can one determine whether a given integer is prime or composite?
- is it possible for given a function to find all the prime numbers?
- are there arbitrarily long sequences of integers, all of which are not primes?

These simple questions have kept mathematicians busy for thousands of years.

3 Working with Primes

By definition, a number greater than one is said to be prime if it only has two divisors, namely one and itself. A quick review of this series of numbers indicates that the higher one counts, the fewer the cases of prime numbers discovered, yet the process continues infinitely.

**Definition 3.1.** A prime number is a natural number greater than 1 that is divisible by no natural numbers other than 1 and itself. A natural number greater than 1 that is not prime is called a composite number.

The difficulty in finding higher value prime numbers has been a persistent problem for mathematicians across the globe, often with news always emerging on the discovery of new, higher value primes.

Note that these are always expressed as Mersenne primes. With mathematicians having agreed that Mersenne primes may not all be prime, the discussion shifts to the question of the possible number of prime numbers that exist out there.

4 Sieve of Eratosthenes

The idea, passing over 1, is to find a prime number and then cross out all of the multiples of this prime number. For example, 2 is prime but every even number is not and so cross all even numbers off the list. Next, 3 is prime and so cross out every multiple of three, because they are not prime. Continue in this fashion, and then the numbers left are the prime numbers. Of course for a given large integer this is not practical, if your time is limited. Since the time of Eratosthenes, sophisticated versions of this algorithm (called the Sieve of Eratosthenes) have achieved new results.

Consider the first 5 rows in the above array. How many primes are there in the first 5 rows? How many in the last five rows? If one carries out the sieve of Eratosthenes between 10,000 and 10,050, you will find that there are just 4 prime numbers. Can we find 5 rows where there are no prime numbers? What is the last prime number?

4.1 Limits of the Sieve of Eratosthenes

As you may have noticed from the previous paragraph, the number of prime numbers tends to decrease as one counts higher. This means that it becomes increasingly difficult to manually employ the sieve of Eratosthenes as the value of interest increases.

While you may have noticed how difficult it is to find the four prime numbers that exist between 10,000 and 10,050, it is relatively easy to do so using an algorithm. Such algorithms employ the segmented sieve approach that works by dividing the range of interest into segments, each of size the square root of the range. The process, however, is equally time consuming.

5 Prime Divisors

The prime number theorem describes the distribution of prime numbers among the integers, and argues that for every integer \( N \) that is large enough, there exists another integer less than \( N \) that is prime. In others words, it is possible to factor any integer large enough as a product of its factors, with at least one of the factors being prime.

A prime divisor is therefore any prime number that divides \( N \), where \( N \) is any integer greater than 1. Note that just as is the case with finding prime numbers, the process of finding these prime divisors grows increasingly complicated as the value of \( N \) increases.

The following lemma, while known to Euclid, is proven using the (modern) Well-Ordering Axiom.

**Lemma 5.1** (Prime Divisor). Every natural number greater than 1 has a prime divisor.

**Proof.** Assume, for a contradiction, that there exists an natural number greater than 1 that does not have a prime divisor. Then since the set of all natural numbers greater than 1 without a prime divisor is nonempty, the Well-Ordering Axiom states that this set must have a least positive natural number, say \( n \), that does not have a prime divisor and is greater than 1. Since \( n \) does not have a prime divisor and \( n \) divides \( n \), \( n \) must not be prime. Thus, \( n = ab \) and since \( a < n \), \( a \) must have a prime divisor and similarly for \( b \). Therefore, \( n = ab \) must have a prime divisor. This contradiction, leads us to the desired conclusion that every natural number greater than 1 must have a prime divisor. \( \square \)

**Lemma 5.2.** If \( n \) is composite, then \( n \) has a prime factor \( p \) such that \( p \leq \sqrt{n} \).

**Proof.** Since \( n \) is composite there exists integers \( a \) and \( b \) such that \( n = ab \) with \( 1 < a \leq b < n \). Suppose \( a > \sqrt{n} \). Then \( b > \sqrt{n} \) and so \( n = ab > \)
\[ \sqrt{n} \sqrt{n} = n, \] which means it fact, \( a \leq \sqrt{n}. \) By Lemma 5.1, \( a \) has a prime divisor, say \( p. \) Hence \( n = ab = (pk)b \) for some integer \( k. \) Therefore, \( p \) is a prime divisor of \( n \) with \( p \leq a \leq \sqrt{n} \) as needed.

6 Infinitude of Primes

Here are the prime numbers less than 1000.

\[
\begin{align*}
2 & \quad 3 & \quad 5 & \quad 7 & \quad 11 & \quad 13 & \quad 17 & \quad 19 & \quad 23 & \quad 29 \\
31 & \quad 37 & \quad 41 & \quad 43 & \quad 47 & \quad 53 & \quad 59 & \quad 61 & \quad 67 & \quad 71 \\
73 & \quad 79 & \quad 83 & \quad 89 & \quad 97 & \quad 101 & \quad 103 & \quad 107 & \quad 109 & \quad 113 \\
127 & \quad 131 & \quad 137 & \quad 139 & \quad 149 & \quad 151 & \quad 157 & \quad 163 & \quad 167 & \quad 173 \\
179 & \quad 181 & \quad 191 & \quad 193 & \quad 197 & \quad 199 & \quad 211 & \quad 223 & \quad 227 & \quad 229 \\
233 & \quad 239 & \quad 241 & \quad 251 & \quad 257 & \quad 263 & \quad 269 & \quad 271 & \quad 277 & \quad 281 \\
283 & \quad 293 & \quad 307 & \quad 311 & \quad 313 & \quad 317 & \quad 331 & \quad 337 & \quad 347 & \quad 349 \\
353 & \quad 359 & \quad 367 & \quad 373 & \quad 379 & \quad 383 & \quad 389 & \quad 397 & \quad 401 & \quad 409 \\
419 & \quad 421 & \quad 431 & \quad 433 & \quad 439 & \quad 443 & \quad 449 & \quad 457 & \quad 461 & \quad 463 \\
467 & \quad 479 & \quad 487 & \quad 491 & \quad 499 & \quad 503 & \quad 509 & \quad 521 & \quad 523 & \quad 541 \\
547 & \quad 557 & \quad 563 & \quad 569 & \quad 571 & \quad 577 & \quad 587 & \quad 593 & \quad 599 & \quad 601 \\
607 & \quad 613 & \quad 617 & \quad 619 & \quad 631 & \quad 641 & \quad 643 & \quad 647 & \quad 653 & \quad 659 \\
661 & \quad 673 & \quad 677 & \quad 683 & \quad 691 & \quad 701 & \quad 709 & \quad 719 & \quad 727 & \quad 733 \\
739 & \quad 743 & \quad 751 & \quad 757 & \quad 761 & \quad 769 & \quad 773 & \quad 787 & \quad 797 & \quad 809 \\
811 & \quad 821 & \quad 823 & \quad 827 & \quad 829 & \quad 839 & \quad 853 & \quad 857 & \quad 859 & \quad 863 \\
877 & \quad 881 & \quad 883 & \quad 887 & \quad 907 & \quad 911 & \quad 919 & \quad 929 & \quad 937 & \quad 941 \\
947 & \quad 953 & \quad 967 & \quad 971 & \quad 977 & \quad 983 & \quad 991 & \quad 997 
\end{align*}
\]

The following proof of the infinitude of primes is a great example of what is called proof by contradiction. The idea is to suppose that there are finitely many prime numbers, and then use these primes to create another natural number whose prime divisor can not be in the original list of all prime numbers.

**Theorem 6.1.** There are infinitely many primes.

**Proof.** Assume that the prime numbers are listed in ascending order with \( p_1 = 2, \ p_2 = 3, \ p_3 = 5, \) and so on; and assume (for a contradiction) that \( p_k \) is the last prime. Consider the natural number,

\[ P = p_1 p_2 \cdots p_k + 1. \]

Since every positive natural number greater than 1 has a prime divisor, \( P \) has a prime divisor, say \( p_m. \) However, \( p_m \) can not divide \( P \) since \( P \) is of the form, \( P = cp_m + 1. \) Therefore \( p_k, \) the last prime number, cannot exist.

For further reading, excellent textbooks on Elementary Number Theory are [1], [3], and [2].

[1] [https://twitter.com/Dave4Math](https://twitter.com/Dave4Math)
[2] [https://www.dave4math.com](https://www.dave4math.com)
7 Exercises

Exercise 7.1. Determine which of the following integers are prime: 201, 207, 213, 203, 211, 221.

Exercise 7.2. Find the smallest prime in the arithmetic progression \( an + b \).
   1. \( a = 3, b = 1 \),
   2. \( a = 5, b = 4 \),
   3. \( a = 7, b = 12 \),
   4. \( a = 11, b = 16 \).

Exercise 7.3. Using the sieve of Eratosthenes, find the prime numbers less than 200.

Exercise 7.4. Show that \( x^2 - x + 41 \) is prime for all integers \( x \) with \( 0 \leq x \leq 40 \). Show that it is composite for \( x = 41 \).

Exercise 7.5. Show that \( 2x^2 + 11 \) is prime for all integers \( x \) with \( 0 \leq x \leq 10 \). Show that it is composite for \( x = 11 \).

Exercise 7.6. Show that \( 2x^2 + 29 \) is prime for all integers \( x \) with \( 0 \leq x \leq 28 \). Show that it is composite for \( x = 29 \).

Exercise 7.7. It has been conjectured that there are infinitely many primes of the form \( n^2 - 2 \). Exhibit five such examples.

Exercise 7.8. Show that any prime of the form \( 3n + 1 \) is also of the form \( 6m + 1 \).

Exercise 7.9. Show that each integer of the form \( 3n + 2 \) has a prime factor of this form.

Exercise 7.10. Show the only prime \( p \) for which \( 3p + 1 \) is perfect square is \( p = 5 \).

Exercise 7.11. Find all primes that are the difference of the fourth powers of two integers.

Exercise 7.12. Show that no integer of the form \( n^3 + 1 \) is a prime, other than 2.

Exercise 7.13. Prove that all odd primes are either of the form \( 4n + 1 \) or \( 4n - 1 \) for some \( n \in \mathbb{N} \).

Exercise 7.14. Prove that, if \( n \in \mathbb{N} \) is a product of primes of the form \( 4n + 1 \), then \( n \) must be of that form.
Exercise 7.15. Let $Q_n = p_1 p_2 \cdots p_n + 1$ where $p_1, p_2, \ldots, p_n$ are the smallest primes. Determine the smallest prime factor of $Q_n$ for $n = 1, 2, 3, 4, 5, \text{ and } 6$. Do you think that $Q_n$ is prime infinitely often?

Exercise 7.16. Show there are infinitely prime numbers of the form $4k+3$.

Exercise 7.17. Give an example to show that the following conjecture is not true: Every positive integer can be written in the form $p + a^2$, where $p$ is either a prime or 1, and $a \geq 0$.

Exercise 7.18. Another unproven conjecture is that there are an infinitude of primes that are 1 less than a power of 2, such as $3 = 2^2 - 1$. Find four more of these primes.

Exercise 7.19. It has been conjectured that every even integer can be written as the difference of consecutive primes in finitely many ways. For example,

$$6 = 29 - 23 = 137 - 131 = 599 - 593 = 1019 - 1013 = \cdots$$

Express the integer 10 as the difference of two consecutive primes in 15 ways.

Exercise 7.20. Find four primes of the form $2^n + 1$ for $n \in \mathbb{N}$.

Exercise 7.21. Prove that if $2^n + 1$ is prime, then $n = 0$ or $n = 2k$ for some integer $k$.

Exercise 7.22. Prove that $p$ is prime if and only if it has no divisors $d$ that satisfy $1 < d \leq \sqrt{p}$.

Exercise 7.23. Show there are infinitely many primes of the form $6k + 5$.

Exercise 7.24. Show that no integer of the form $n^3 + 1$ is a prime, other than 2.

Exercise 7.25. Explain why $(a, a^2) = a$ where $a$ is a positive integer. Explain why 201 is not a prime. Explain why 11 is a prime number.

References

