2. Primes

Primes.

- A natural number greater than 1 is prime if it cannot be expressed as the product of two smaller natural numbers.
- A natural number greater than 1 that is not prime, and therefore is the product of two smaller natural numbers, is composite.

The study of primes is one of the main focuses of number theory. As we shall prove, every natural number greater than 1 is either prime or it can be expressed as a product of primes. The prime numbers give us a world of questions to explore. We will prove that there are infinitely many primes, but how are they distributed among the natural numbers? How many primes are there less than a natural number $n$? How can we find them? How can we use them? These questions and others have been among the driving questions of number theory for centuries and have led to an incredible amount of beautiful mathematics.

Some of the basic techniques of analysis that arise in this study include: doing an example and then generalizing the method; proving a statement by contradiction, that is, assuming the statement is not true and then logically deducing a contradiction from that (false) assumption, thereby proving that the theorem must be true.

2.1. Theorem. If a natural number $n > 1$ is not prime, then there exists a prime $p$ such that $p|n$.

2.2. Exercise (Sieve of Eratosthenes). Write down all the natural numbers from 1 to 100, perhaps on a $10 \times 10$ array. Circle the number 2, the smallest prime. Cross off all numbers divisible by 2. Circle 3, the next number that is not crossed out. Cross off all larger numbers that are divisible by 3. Continue to circle the smallest uncrossed out number and cross out its multiples. (a) Why are the circled numbers all the primes less than 100? (b) For each natural number $n$, $\pi(n)$ denotes the number of primes less than or equal to $n$. Graph $\pi(n)$ for $n = 1, 2, \ldots, 100$. (c) Make a guess about approximately how large $(n)$ is relative to $n$. In particular, do you suspect that $\frac{\pi(n)}{n}$ is generally an increasing function or a decreasing function, and do you suspect that it approaches some specific number as a limit as $n$ goes to infinity?

2.3. Theorem. A natural number $n$ is prime if and only if for all primes $p \leq \sqrt{n}$, $p$ does not divide $n$.

2.4. Exercise. Use the preceding theorem to verify that 101 is prime.
2.5. **Theorem (Fundamental Theorem of Arithmetic (existence part)).** Every natural number greater than 1 is either a prime number or it can be expressed as a finite product of prime numbers, that is, for every natural number \( n \) greater than 1, there exist distinct primes \( p_1, p_2, \ldots, p_m \) and natural numbers \( r_1, r_2, \ldots, r_m \) such that \( n = p_1^{r_1} p_2^{r_2} \cdots p_m^{r_m} \).

2.6. **Lemma.** Let \( p \) and \( q_1, q_2, \ldots, q_n \) all be primes and let \( k \) be a natural number such that \( p^k = q_1 q_2 \cdots q_n \). Then \( p = q_i \) for some \( i \).

2.7. **Theorem (Fundamental Theorem of Arithmetic (uniqueness part)).** Let \( n \) be a natural number. Let \( \{p_1, p_2, \ldots, p_m\} \) and \( \{q_1, q_2, \ldots, q_s\} \) be sets of primes with \( p_i \neq p_j \) if \( i \neq j \) and \( q_i \neq q_j \) if \( i \neq j \). Let \( \{r_1, r_2, \ldots, r_m\} \) and \( \{t_1, t_2, \ldots, t_s\} \) be natural numbers such that \( p_1^{r_1} p_2^{r_2} \cdots p_m^{r_m} = q_1^{t_1} q_2^{t_2} \cdots q_s^{t_s} \). Then \( m = s \) and \( \{p_1, p_2, \ldots, p_m\} = \{q_1, q_2, \ldots, q_s\} \), that is, the sets of primes are equal but they may not be in the same order, so \( p_i \) may or may not equal \( q_i \). Moreover, if \( p_i = q_j \), then \( r_i = t_j \). In other words, if we express the same natural number as a product of powers of distinct primes, then the expressions are identical except for the ordering of the factors.

Putting the existence and uniqueness parts together, we get the whole formulation of the Fundamental Theorem of Arithmetic.

**Fundamental Theorem of Arithmetic.** Every natural number greater than 1 is either a prime number or it can be expressed as a finite product of prime numbers and the expression is unique up to the order of the factors.

2.8. **Question.** Express \( n = 12! \) as a product of primes.

2.9. **Question.** Determine the number of 0’s at the end of \( 25! \)

The Fundamental Theory of Arithmetic says that for \( n > 1 \) there exist distinct primes \( \{p_1, p_2, \ldots, p_m\} \) and natural numbers \( \{r_1, r_2, \ldots, r_m\} \) such that \( n = p_1^{r_1} p_2^{r_2} \cdots p_m^{r_m} \) and, moreover, the factorization is unique up to order. We will say that \( p_1^{r_1} p_2^{r_2} \cdots p_m^{r_m} \) is the unique prime factorization of \( n \).

2.10. **Theorem.** Let \( a \) and \( b \) be natural numbers greater than 1 and let \( p_1^{r_1} p_2^{r_2} \cdots p_m^{r_m} \) be the unique prime factorization of \( a \) and let \( q_1^{t_1} q_2^{t_2} \cdots q_s^{t_s} \) be the unique prime factorization of \( b \). Then \( a | b \) if and only if for all \( i \leq m \) there exists a \( j \leq s \) such that \( p_i = q_j \) and \( r_i \leq t_j \).

2.11. **Theorem.** If \( a \) and \( b \) are natural numbers and \( a^2 | b^2 \), then \( a | b \).
2.12. **Question.** Find \((3^{14}7^{22}11^517^3, 5^211^413^817)\).

2.13. **Question.** Find \(\text{lcm}(3^{14}7^{22}11^517^3, 5^211^413^817)\).

2.14. **Conjecture.** Make a conjecture that generalizes the ideas you used to answer the two previous questions.

2.15. **Question.** Do you think this method is always a better or always a worse method than using the Euclidean Algorithm to find \((a, b)\)? Why?

2.16. **Theorem.** Let \(a, b,\) and \(n\) be integers. If \(a|n, b|n,\) and \((a, b) = 1,\) then \(ab|n.\)

2.17. **Theorem.** Let \(p\) be a prime and \(a\) be an integer. If \(p\) does not divide \(a,\) then \((a, p) = 1.\)

2.18. **Theorem.** Let \(p\) be a prime and \(a\) and \(b\) be integers. If \(p|ab,\) then \(p|a\) or \(p|b.\)

2.19. **Theorem.** Let \(a, b,\) and \(c\) be integers. If \((b, c) = 1,\) then \((a, bc) = (a, b)(a, c).\)

2.20. **Theorem.** Let \(a, b,\) and \(c\) be integers. If \((a, b) = 1\) and \((a, c) = 1,\) then \((a, bc) = 1.\)

2.21. **Theorem.** Let \(a, b\) be integers. If \((a, b) = d,\) then \((\frac{a}{d}, \frac{b}{d}) = 1.\)

2.22. **Theorem.** Let \(a, b, u,\) and \(v\) be integers. If \((a, b) = 1, u|a,\) and \(v|b,\) then \((u, v) = 1.\)

2.23. **Theorem.** For all natural numbers \(n,\) \((n, n + 1) = 1.\)

2.24. **Theorem.** Let \(k\) be a natural number. Then there exists a natural number \(n\) (which will be larger than \(k\)) such that no natural number less than \(k\) and greater than 1 divides \(n.\)

2.25. **Theorem (Infinitude of Primes Theorem).** There are infinitely many prime numbers.

2.26. **Question.** After you have devised a proof or proofs for 2.25, what were the most clever or most difficult parts of your arguments?

2.27. **Question.** If you are given \(n + 1\) natural numbers less than or equal to the natural number \(2n,\) is some pair necessarily relatively prime?

2.28. **Theorem.** There exist arbitrarily long sequences of composite numbers. That is, for any natural number \(n,\) there exists a run of \(n\) consecutive composite (that is, non-prime) natural numbers.
Definitions. A *rational number* is a number that can be written as \( \frac{a}{b} \) where \( a \) and \( b \) are integers (\( b \neq 0 \)). A real number that is not rational is *irrational*.

The Fundamental Theorem of Arithmetic can be used to prove that certain equations do not have integer solutions.

2.29. **Theorem.** There do not exist natural numbers \( m \) and \( n \) such that \( 7m^2 = n^2 \).

2.30. **Theorem.** \( \sqrt{7} \) is irrational, that is, there do not exist natural numbers \( n \) and \( m \) such that \( \sqrt{7} = \frac{n}{m} \).

2.31. **Question.** For what other numbers can you prove their irrationality? Make and prove the most general conjecture you can.

2.32. **Theorem.** If \( r_1, r_2, \ldots, r_m \) are natural number and each one is congruent to 1 (mod 4), then \( r_1r_2\ldots r_m \) is also congruent to 1 (mod 4).

2.33. **Theorem** (Infinitude of \( 4k+3 \) Primes Theorem). There are infinitely many prime numbers that are congruent to 3 (mod 4).

In fact, the following much more general theorem is true, however, its proof is quite difficult and we will not attempt it in this course:

**Infinitude of \( ak+b \) Primes Theorem.** If \( a \) and \( b \) are relatively prime, then there are infinitely many integers \( k \) for which \( ak+b \) is prime.

*Mersenne primes.* A Mersenne prime is a prime of the form \( 2^p - 1 \) where \( p \) is a prime.

2.34. **Question.** What is \( \frac{2^m-1}{x-1} \) if \( x \neq 1 \)?

2.35. **Theorem.** If \( n \) is a natural number and \( 2^n - 1 \) is prime, then \( n \) must be a prime.

2.36. **Question.** Find the first few Mersenne primes.

2.37. For extra credit, an A in the class, and a Ph.D. in mathematics, prove that there are infinitely many Mersenne primes or prove that there aren’t.

**Distribution of primes.** How are the primes distributed among the natural numbers? Is there some pattern to their distribution? There are infinitely many primes, but how rare are they among the numbers? What proportion of the natural numbers are prime numbers? To explore these questions, the best way to start is to look at the natural numbers and the
primes among them. Here then are the first few natural numbers with the primes printed in bold:

\[
1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11, 12, 13, 14, 15, 16, 17, 18, 19, 20, 21, 22, 23, 24, \ldots
\]

Out of the first 24 natural numbers, 9 of them are primes. We see that \(9/24 = .375\) of the first 24 natural numbers are primes—that’s just a little over one third. We saw how this fraction changes as \(n\) increases in the Sieve of Eratosthenes exercise.

Before high-speed computers were available, calculating (or just estimating) the proportion of prime numbers in the natural numbers was a difficult task. In fact, years ago “computers” were in fact humans who did computations—such people were amazingly accurate, but required a great deal of time and dedication to accomplish what today’s computers can do in seconds. An eighteenth-century Austrian arithmetician by the name of J.P. Kulik spent 20 years of his life creating, by hand, a table of the first 100 million primes. His table was never published and sadly the volume containing the primes between 12,642,600 and 22,852,800 has since disappeared.

Nowadays, there are programs that compute the number of primes less than \(n\), denoted \(\pi(n)\), for increasingly large values of \(n\) and print out the proportion: \(\pi(n)/n\). If we examine the results, we notice that the proportion of primes slowly goes downward. That is, the percentage of numbers less than a million that are prime is smaller than the percentage of numbers less than a thousand that are prime. The primes, in some sense, get sparser and sparser among the bigger numbers.

In the early 1800’s, well before computers were even imagined, Karl Friedrich Gauss, known by many as the Prince of Mathematics, and A.-M. Legendre made an insightful observation about the primes. They noticed that even though primes do not appear to occur in any predictable pattern, the proportion of primes is related to the natural logarithm.

Gauss and Legendre conjectured that the proportion of the number of primes among the first \(n\) natural numbers is approximately \(1/\ln(n)\). Below is a chart of the number of primes up to \(n\), the proportions of primes, and a comparison with \(1/\ln(n)\).

17
\begin{tabular}{|c|c|c|c|c|}
\hline
n & \pi(n) & Prop. of primes: $1/\ln(n)$ & $\pi(n)/n - 1/\ln(n)$ & $\pi(n)/n$
\hline
10 & 4 & .4 & .43429... & -.03429...
100 & 25 & .25 & .21714... & .03285...
1000 & 168 & .168 & .14476... & .02323...
10000 & 1229 & .1229 & .10857... & .01432...
100000 & 9592 & .09592 & .08685... & .00906...
1000000 & 78498 & .078498 & .07238... & .00611...
10000000 & 664579 & .0664579 & .06204... & .00441...
100000000 & 5761455 & .05761455 & .05428... & .00332...
1000000000 & 50847534 & .050847534 & .04825... & .00259...
\hline
\end{tabular}

Notice how the last column seems to be getting closer and closer to zero—that is, the proportion of primes in the first $n$ natural numbers is approximately $1/\ln(n)$ and the fraction $\pi(n)/n$ is becoming increasingly closer to $1/\ln(n)$ as $n$ grows without bound.

**The Prime Number Theorem.** As $n$ approaches infinity, the number of prime numbers less than or equal to $n$ approaches $n/\ln(n)$. Specifically, $\lim_{n \to \infty} (\pi(n)/n - 1/\ln(n)) = 0$.

The proofs of this theorem are difficult. If you prove it independently, you don’t have to take the final.

Here are two famous open questions about prime numbers. If you solve them, you don’t have to take the final.

**The Twin Prime Question.** Are there infinitely many pairs of prime numbers that differ from one another by two? (11 and 13, 29 and 31, 41 and 43 are examples of some such pairs.)

**The Goldbach Question.** Can every positive, even number greater than 2 be written as the sum of two primes? (Pick some even numbers at random and see whether you can write them each as a sum of two primes.)

The Goldbach Conjecture has been verified by computer for all even numbers up to 400,000,000,000,000. As the even numbers get larger, there seem to be more ways to write them as a sum of two primes. For example, the number 100,000,000 can be written as the sum of two primes in 219,400 different ways.