Section 1.3. Listing the Primes

Note. In this section we consider algebraic functions that generate prime numbers (with some caveats) and consider distributions of primes. We prove Bertrand's "Postulate," Fermat's Little Theorem, define Mersenne primes, and prove a theorem of Zsigmondy.

Note. The "Sieve of Eratosthenes" involves the elimination of composite numbers by first removing multiples of 2 greater than 2, then removing multiples of 3 greater than 3, then removing multiples of 5 greater than 5, etc. If all multiples of primes less than or equal to n have been removed, then all numbers less than n^2 which remain must be prime. Wikipedia has a nice janimated GIF of the Sieve of Eratosthenes (accessed 4/17/2022) which finds all prime numbers between 2 and 120 by eliminating multiples of 2, 3, 5, 7, and 11. For biographical information of Eratosthenes of Cyrene, see my online notes for Elementary Number Theory (MATH 3120) on Section 2. Unique Factorization. The generation of tables of primes was instrumental in the first conjectures on the Prime Number Theorem by Adrien-Marie Legendre in 1797–98 and by Carl Friedrich Gauss in 1792–93 (though Gauss, as was his habit, never published this). For details, see my online notes on Supplement. The Prime Number Theorem—History. We present the Prime Number Theorem here as Theorem 8.1.

Note. Leonhard Euler (April 15, 1707–September 18, 1783) observed that the polynomial n^2+n+41 gives distinct primes for integers $n = 0, 1, 2, \ldots, 39$ (This is

Everest and Ward's Example 1.7). He gave this in his 1772 *Nouveaux Mémoires de lAcadémie royale des Sciences*, Berlin (page 36). This is called a prime generating polynomial. For other examples, see Wolfram's "Prime-Generating Polynomial" website (accessed 4/17/2022). It can be shown that no polynomial with integer coefficients can take on only prime values on the natural numbers. This is Everest and Ward's Exercise 1.6(a) and is given in Elementary Number Theory (MATH 3120) as Theorem 22.C of Section 22. Formulas for Primes. However, there is a polynomial function of degree 25 in 26 variables such that the set of positive values of the function (for nonnegative values of the variables) is the set of prime numbers. Details are given at the end of the Elementary Number Theory notes just mentioned. However this polynomial, as well as other such functions, is useless in actually generating prime numbers. We'll present a prime generating formula below (in Corollary 1.10) and see that it requires the use of a parameter θ; the existence of θ will be established, though the value of θ will remain undetermined (and hence the formula is not useful). We begin our approach with a lemma, then Bertrand's Postulate, which will lead to the formula. The following lemma is equivalent to Lemma 22.E in the preciously mentions notes for Elementary Number Theory.

Lemma 1.8. For any $n \geq 1$, $\sum_{p \leq n} \log p < 2n \log 2$.

Note. We now present Bertrand's Postulate, so named because it was first conjectured in 1845 by French mathematician Joseph Bertrand (March 11, 1822–April 5, 1900) and verified by him for parameter n up to three million (thus the "pos-

tulate" status). It was proved by Pafnuty Chebyshev (May 16, 1821–December 8, 1894) in his "Mémoire sur les nombres premiers," *Journal de mathématiques pures et appliquées, Série 1*, 366–390 (1852). A copy of Chebyshevs paper is available online at MathDocs website (accessed 4/17/2022).

Theorem 1.9. Bertrand's Postulate.

If $n \geq 1$, then there is at least one prime p with the property that $n < p \leq 2n$.

Note. Notice that Bertrand's Postulate deals, in a sense, with the distribution of prime numbers (as does the Prime Number Theorem). If we list the primes in order as $p_1, p_2, p_3, \ldots$ then we have that $p_{n+1} < 2p_n$ for all $n \in \mathbb{N}$. One might think that we can put a bound on the gap between consecutive prime numbers, but this is not the case. It can be shown that for any $N > 0$ there are consecutive prime numbers p_i and p_{i+1} such that $p_{i+1} - p_i \geq N$. This is Exercise 1.1.2 in Graham Jameson's *The Prime Number Theorem*, London Mathematical Society Student Texts, Series Number 53, Cambridge University Press (2003). I have some notes online based on this book at Prime Number Theorem Class Notes.

Note/Definition. Bertrand's Postulate can be used to give another proof that there are infinitely many primes, since each interval of the form $(n, 2n]$ contains a prime for every $n \geq 1$. In fact, we have that the interval

$$(1, 2^N] = (1, 2] \cup (2, 4] \cup (4, 8] \cup \cdots \cup (2^{N-1}, 2^N]$$

contains at least N primes. The *prime counting function* π is defined as $\pi(X) =$

$|\{p \leq X \mid p \in \mathbb{P}\}|$. Bertrand's Postulate then gives us a lower bound on $\pi(X)$ in the sense that $\pi(2^N) > N$. This implies that $\pi(X) > C \log X$, for some positive constant C, infinitely often (namely, when $X = 2^N$ for $N \in \mathbb{N}$).

Note. We now give a prime generating function. This appears in Elementary Number Theory (MATH 3120) as Theorem 22.3 in Section 22. Formulas for Primes. It is an interesting result, but not a useful one. Parameter θ can be used to generate arbitrarily large primes, but the value of θ depends on knowing arbitrarily large prime. So this (nor any other known technique) can be used to generate prime numbers. Our formula uses the "rounding down" floor function $\lfloor x \rfloor$.

Corollary 1.10. There exists a real number θ with the property that $\left\lfloor 2^{2^{2^{\cdot^{\cdot^{\cdot^{\theta}}}}}} \right\rfloor$ is a prime number for any number of iterations of the exponential.

Revised: 4/17/2022