Section 22. Formulas for Primes

Note. In this section we consider, in a sense, the distribution of primes. We consider primes in arithmetic progression, and look for functions that generate primes. We also prove Bertrand's Theorem, which state that for any $n \geq 2$, there is a prime p between n and $2n$.

Note. Since the Fundamental Theorem of Arithmetic/Unique Factorization Theorem (Theorem 2.2) tells us that prime numbers are the "building blocks" of all integers, we are interested is finding prime numbers! One might fantasize about a function $p(n)$ that produces for each $n \in \mathbb{N}$, then nth prime. Dudley declares such a function "probably beyond all reason" (see page 173). Perhaps, then, there is a function (represented by a formula) that produces nothing but primes? We will show below that no polynomial function will work for this (in Theorem 22.C below). First, if we try a first degree polynomial function $f(n) = an + b$ then we see that the resulting primes would be evenly spaced; that is, they would form an arithmetic progression with difference a. Some examples of finite arithmetic progressions of prime numbers are: 3, 5, 7 (where $a = 2$); 7, 37, 67, 127, 157 (where $a = 30$); and 199, 409, 619, 829, 1039, 1249, 1459, 1669, 1879, 2089 (where $a = 210$). In fact, such an arithmetic progression of prime numbers *must* be finite, as we now prove.

Theorem 22.A. An arithmetic progression of prime numbers must be finite in length.

Note. Dudley states that (see page 173) "it is not known if there exist arbitrarily long arithmetic progressions of primes." But Dudley's book was written in 1978. In 2008 Ben Green and Terence Tao published: "The primes contain arbitrarily long arithmetic progressions," *Annals of Mathematics*, **167**(2), 481–547 (2008). A copy is available online on the Annals of Mathematics webpage (accessed 3/9/2022).

Note. We now turn our attention from arithmetic progressions or primes, to the number of primes in the sequence $f(n) = an + b$. German mathematician Peter Lejeune Dirichlet (February 13, 1805–May 5, 1859) proved in 1837:

Theorem 22.B. Dirichlet's Theorem.
For positive integers a and b, where $(a, b) = 1$, there are infinitely many primes of the form $an + b$, where n is a positive integer. That is, there are infinitely many primes that are congruent to b modulo a.

Dirichlet's proof was inspired by work done by Euler in the 1700s which related the Riemann Zeta function to the distribution of primes. Dirichlet used "L-series" and published his result in "Proof of the theorem that every unbounded arithmetic progression, whose first term and common difference are integers without common factors, contains infinitely many prime numbers," *Abhandlungen der Königlichen Preußischen Akademie der Wissenschaften zu Berlin*, **48**, 45-71 (1837). A proof can be found in Graham Everest and Thomas Ward's *An Introduction to Number Theory*, NY: Springer (2005) in Chapter 10. Primes in an Arithmetic Progression. I am preparing online notes for ETSU's Number Theory (MATH 5070; a class that has been "mothballed" since 2015) based on this book.

Note 22.A. Notice that the condition $(a, b) = 1$ is necessary since, for example, the sequence $\{6n+3\}$ contains one prime and the sequence $\{6n+4\}$ contains no primes. In some cases, it is easy to show that the sequence contains an infinite number of primes. Consider the sequence $\{3n+2\}$ and ASSUME that it only contains a finite number of primes, $p_1, p_2, \ldots, p_k$. Notice that the sequence $\{3n + 2\}$contains all natural numbers that are 2 (mod 3), and so it contains all primes that are 2 (mod 3). Let $N = p_1 p_2 \cdots p_k$. If $N \equiv 1(\text{ mod } 3)$, then $N + 1 \equiv 2 \text{ (mod 3)}$ and so $N + 1$ must have at least one prime divisor congruent to 2 (mod 3) (it can't have a divisor that is 0 (mod 3) or else it we would have $N + 1 \equiv 0 \text{ (mod 3)}$, and it all of it's divisors are 1 (mod 3) then we would have $N + 1 \equiv 1 \text{ (mod 3)}$). But $N + 1 \equiv 1 \text{ (mod } p_i)$ for each $i \in \{1, 2, \ldots, k\}$, so the prime divisor of $N + 1$ cannot be in the list of 2 (mod 3) primes $p_1, p_2, \ldots, p_k$. If $N \equiv 2 \text{ (mod 3)}$, then $N + 3 \equiv 2 \text{ (mod 3)}$, and $N + 3$ must have a prime divisor congruent to 2 (mod 3) (similar to above). But $N + 3 \equiv 3 \text{ (mod } p_i)$ for each $i \in \{1, 2, \ldots, k\}$, so the prime divisor of $N + 3$ cannot be in the list of 2 (mod 3) primes $p_1, p_2, \ldots, p_k$. So in both cases, we have a CONTRADICTION, so that the assumption that there are only finitely many primes in the sequence $\{3n+2\}$ is false and hence there are infinitely many primes in the sequence.

Theorem 22.C. If $f(n) = a_k n^k + a_{k-1} n^{k-1} + \cdots + a_2 n^2 + a_1 n + a_0$ is a polynomial function with integer coefficients and if r is such that $f(r) \equiv 0 \text{ (mod } p)$ for some p, then $f(r + mp) \equiv f(r) \equiv 0 \text{ (mod } p)$ for all $m \in \mathbb{N}$. That is, no polynomial can have only prime values.

Note. Euler observed that the polynomial n^2+n+41 gives distinct primes for integers $n = 0, 1, 2, \ldots, 39$. He gave this in his 1772 *Nouveaux Mémoires de l'Académie royale des Sciences*, Berlin (page 36). This is called a *prime generating polynomial*. For other examples, see Wolfram's "Prime-Generating Polynomial" website (accessed 3/9/2022).

Note 22.B. We make a passing comment that we can construct a polynomial (maybe not with integer coefficients) that "generates" as many (but finite) prime numbers as we want. Dudley mentions (on page 174), for example, that with

$$60f(x) = 7x^5 - 85x^4 + 355x^3 - 575x^2 + 418x + 180$$

we have $f(0) = 3$, $f(1) = 5$, $f(2) = 7$, $f(3) = 11$, $f(4) = 13$, and $f(5) = 17$. So the 5th degree polynomial $60f(x)$ generates the 6 consecutive prime numbers given. This takes advantage of the fact that for $d + 1$ points in the Cartesian plane with different x values, we can find a degree (at most) d polynomial that passes through each of these points. These polynomials are called *Lagrange polynomials*; for details, see my online notes for Numerical Analysis (MATH 4257/5257) on Section 3.1. Interpolation and the Lagrange Polynomial. Though a Lagrange polynomial will pass through the given points, it will oscillate wildly in the process and will not be useful for interpolation or extrapolation.

Note. As opposed to polynomials, we might try exponential functions. We can combine exponential functions with the greatest integer function. For example, $f(n) = [(3/2)^n]$ is prime for $n = 2$, 3, 4, 5, 6, and 7 since these give 2, 3, 5, 7, 11, and 17, respectively. Dudley observes on page 175: "No one has proved that a formula like $f(n) = [\theta^n]$ cannot always give a prime. Nor is it known whether $[\theta^n]$ can be prime infinitely often. Such questions seem hopelessly difficult." This being said, the next result, due to W. H. Mills in "A Prime-Representing Function," *Bulletin of the American Mathematical Society*, **53**(6), 604 (June 1947) (and available online on the Project Euclid webpage) appears very impressive!

Theorem 22.1. There is a real number θ such that $[\theta^{3^n}]$ is a prime for all $n \in \mathbb{N}$.

Note. Though the result appears impressive, as we will see in the proof below it is not of any practical use. The construction of θ depends on being able to recognize arbitrarily large primes, and the point of finding the formula is to use it to generate arbitrarily large primes! For the proof, we need two results from Analysis 1 (MATH 4217/5217). We state them here as lemmas. Both follow from the fact that a bounded monotone sequence of real numbers converges (see my online notes for Analysis 1 on Section 2.1. Sequences of Real Numbers and Theorem 2-6).

Lemma 22.A. If a sequence (of real numbers) $u_1, u_2, \ldots, u_n, \ldots$ is bounded above and nondecreasing, then it has limit θ as n increases without bound; that is, $\lim_{n\to\infty} u_n = \theta$.

Lemma 22.B. If a sequence (of real numbers) $v_1, v_2, \ldots, v_n, \ldots$ is bounded below and nonincreasing, then is has a limit φ as n increases without bound; that is, $\lim_{n\to\infty} v_n = \varphi$.

Note. We take one more result as given. It is proved in W. H. Mills' one page 1947 paper using another inequality that establishes the existence of integer A referenced in the result.

Theorem 22.D. (Mills, 1947). There is an integer A such that if $n > A$, then there is a prime p such that $n^3 < p < (n+1)^3 - 1$.

Note. We are now ready to give a proof of Theorem 22.1.

Note. Now that we have been through the proof, we see that it is based on the creation of an infinite, strictly increasing sequence sequence of prime numbers $\{p_n\}$ (notice that we are not saying that this is *all* prime numbers, but just an increasing sequence of distinct primes). The sequence is used to define a bounded increasing sequence $\{u_n\} = \{p_n^{3^{-n}}\}$ that converges to θ. We know of the existence of the primes p_n by Theorem 22.D, but we have no idea what the primes are (nor do we have any idea what parameter A of Theorem 22.D is). So this is not a practical way to generate an infinite number of primes, since it requires an infinite number of known primes first!

Note. The next result is commonly known as Bertrand's Postulate, Bertrand's Theorem, the Bertrand-Chebyshev Theorem, or Chebyshev's Theorem. It was first conjecture 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 "postulate" 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 Chebyshev's paper is available online at MathDocs website (accessed 3/10/2022).

Theorem 22.2. Bertrand's Theorem.
For all integers $n \geq 2$, there is a prime p such that $n < p < 2n$.

Note 22.C. We break up the proof of Bertrand's Theorem given by Dudley. First, notice that the sequence of primes 2, 3, 5, 7, 13, 23, 43, 83, 163, 317, 631, 1259, 2503, 9973 shows that Bertrand's Theorem holds for $n \leq 9973$ since each prime in the sequence is less than twice the one before it. Next, we present two lemmas.

Lemma 22.E. For $n \geq 2$, we have $\prod_{p \leq n} p \leq 2^{2n}$ where p is prime.

Lemma 22.F. For $n \geq 1$, we have $\binom{2n}{n} \geq \dfrac{2^{2n}}{2n}$.

Note. We are now ready to give a proof of Bertrand's Theorem (Theorem 22.2).

Note. In Theorem 22.1, we proved the existence of a formula that generates primes (but with the warnings of its uselessness, discussed above). The proof depended on a result we did not prove, namely Theorem 22.D of Mills (1947). We now state a related result, the proof of which is based only on results proved in these notes.

Theorem 22.3. There exists a real number θ such that $[2^\theta]$, $[2^{2^\theta}]$, $[2^{2^{2^\theta}}]$, ... are all prime.

Note. Recall that Wilson's Theorem (Theorem 6.2) states: Positive integer p is prime if and only if $(p-1)! \equiv -1 \pmod{p}$. That is, $(p-1)!+1 \equiv 0 \pmod{p}$ or $\dfrac{(p-1)!+1}{p}$ is an integer if and only if p is prime. So we can define $f(n) = \cos^2 \pi \left(\dfrac{(n-1)!+1}{n} \right)$ and then $f(n) = 1$ if and only if n is prime (and $f(n) < 1$ if n is composite). So we can use f to count primes, and we have $\pi(x) = \sum_{2 \le n \le x} [f(n)]$.

Note. Dudley ends his book with a "striking result," which is also based on Wilson's Theorem. The result appeared in James P. Jones, Daihachiro Sato, Hideo Wada and Douglas Wiens' "Diophantine Representation of the Set of Prime Numbers," *The American Mathematical Monthly*, **83**(6), 449–464 (June-July, 1976). A copy of the paper can be found on The University of Maryland webpage of Chris Laskowski and it is also available through JSTOR (though this will require you to log in with your ETSU username and password). The result is:

Theorem (Jones et al). The set of prime numbers is identical with the set of positive values taken on by the following polynomial of degree 25 in the 26 variables $x_1, x_2, \ldots, x_{26}$ as the variables range over the nonnegative integers:

$$(x_{11}+2)\{1-[x_{23}x_{26}+x_8+x_{10}-x_{17}]^2$$
$$-[(x_7x_{11}+2x_7+x_{11}+1)(x_8+x_{10})+x_8-x_{26}]^2$$
$$-[2x_{14}+x_{16}+x_{17}+x_{26}-x_5]^2$$
$$-[16(x_{11}+1)^3(x_{11}+2)(x_{14}+1)^2+1-x_6^2]^2$$
$$-[x_5^3(x_5+2)(x_1+1)^2+1-x_{15}^2]^2$$
$$-[(x_1^2-1)x_{25}^2+1-x_{24}^2]^2-[16x_{18}^2x_{25}^4(x_1^2-1)+1-x_{21}^2]^2$$
$$-[(x_1+x_{21}^2(x_{21}^2-x_1)^2-1)(x_{14}+4x_4x_{25})^2+1-(x_{24}+x_3x_{21})^2]^2$$
$$-[x_{14}+x_{12}+x_{22}-x_{25})^2-[(x_1^2-1)x_{12}^2+1-x_{13}^2]^2$$
$$-[x_1x_9+x_{11}+1-x_{12}-x_9]^2$$
$$-[x_{16}+x_{12}(x_1-x_{14}-1)+x_2(2x_1x_{14}+2x_1-x_{14}^2-2x_{14}-2)-x_{13}]^2$$
$$-[x_{17}+x_{25}(x_1-x_{16}-1)+x_{19}(2x_1x_{16}+2x_1-x_{16}^2-2x_{16}-2)-x_{24}]^2$$
$$-[x_{26}+x_{16}x_{12}(x_1-x_{16})+x_{20}(2x_1x_{16}-x_{16}^2-1)-x_{16}x_{13}]^2\}.$$

Revised: 4/17/2022