POLYNOMIAL PRIME GENERATING FUNCTIONS

OLGA RADKO MATH CIRCLE
ADVANCED 3
JANUARY 10, 2021

Introduction

The prime numbers underlie much of early and advanced mathematics. (Oh boy...here we go again with primes.) Thus it is natural to try to predict when prime numbers will occur. Mathematicians have made estimates about prime number spacing, but we have decided that the distribution of prime numbers is fairly random. One (not me) might ask: Is there a function with natural number inputs whose outputs are the prime numbers? In this worksheet, we will explore the importance and limitations of a few examples of prime generating polynomials.

Can Polynomials Generate Prime Numbers?

In 1772, Euler noticed that, for n a natural number, the function $f(n) = n^2 + n + 41$ generates a good number of primes. However, we will show in this section that Euler was wasting his time. In other words, polynomials are not going to be perfect prime generating functions.

Problem 1. (a) Compute $f(0)$, $f(1)$, and $f(2)$. Are they prime numbers? Make a guess as to how long f outputs prime numbers.
(b) Show that f is increasing on natural number inputs.
(c) Does f skip any prime numbers? If so, find the first instance of a missing prime.
(d) Show that $f(40)$ is not prime without computing the actual output.

It turns out that f is prime for all $0 \leq n \leq 39$. After that, it is composite frequently. If you test polynomials for their ability to generate prime numbers, you'll find that they often output composite numbers. (So why are we still doing this worksheet?) The following exercise will make this claim rigorous.

Problem 2. We will show that no non-constant polynomial f can be prime for all natural number inputs.
(a) Assume that f is a polynomial that is prime for all natural inputs. Let $p = f(1)$, which is assumed to be prime. Show that $f(1 + kp)$ is divisible by p for all natural numbers k.
(b) What is $f(1 + kp)$ for all natural numbers k?
(c) Conclude that f must be constant.

Dirichlet's Theorem

Even though polynomials cannot always output prime numbers, there are many instances of polynomials that generate infinitely many prime numbers. As a simple example, take $f(n) = n$. Since f generates all natural numbers, it generates all prime numbers. (Wow, that was such a sick example. I am fully into this section now.)

Recall that the *greatest common divisor* of two integers a and b is the largest integer that divides both a and b. Two numbers are *relatively prime* if their greatest common divisor is 1. The following theorem is an important result in number theory.

Theorem 1 (Dirichlet's Theorem)**.** For any two relatively prime numbers a and b, the function $f(n) = an + b$ will be prime infinitely often.

Problem 3. (a) Explain why Dirichlet's Theorem holds for $a = 2$ and $b = 1$.
(b) Prove that Dirichlet's Theorem holds for $a = 4$ and $b = 3$.

(c) (Challenge) Prove that Dirichlet's Theorem holds for $a = 8$ and $b = 3$. (Hint: Try a quadratic formulation.)

(Okay, maybe I misjudged the section.) A result like Dirichlet's Theorem is not known for polynomials of higher degrees although there is a conjecture. The next problem develops the key pieces of the conjecture.

Problem 4. Assume that f is a polynomial where $f(n)$ is a prime number infinitely often.

(a) Show that the leading coefficient of f is positive.
(b) Show that f cannot be factored as the product of two integer coefficient polynomials.
(c) Show that the greatest common divisor of $f(1), f(2), f(3), \ldots$ is 1. Note that this condition implies the coefficients of f have greatest common divisor 1.

Problem 5. In Dirichlet's Theorem, the coefficients of the polynomial only needed to be relatively prime. However, in Problem 4, condition (c) is stronger than just having the coefficients have greatest common divisor 1. Show that $f(n) = n^2+n+2$ does not generate infinitely many primes even though its coefficients are relatively prime.

Conjecture 1 (Bunyakovsky's Conjecture)**.** A polynomial that satisfies (a), (b), and (c) in Problem 4 will generate infinitely many primes.

Divisibility Results

Since it is apparently difficult to say when polynomials generate infinitely many primes, we will weaken the question in the next problem.

Problem 6. Show that for a non-constant polynomial f, the set of prime numbers dividing $f(n)$ for some natural number n is infinite.

(a) Suppose that the set of prime numbers dividing $f(n)$ for some natural number n is finite, say $p_1, ..., p_k$. Let $f(x) = a_n x^n + ... + a_1 x + a_0$. Show that there is no natural number m such that $f(m) = 0$, that is, f has no natural roots. Conclude that $a_0 \neq 0$.
(b) Show that a_0 is a product of the prime numbers in our set, $a_0 = p_1^{\alpha_1} \cdots p_k^{\alpha_k}$.
(c) Show that $a_0 \neq 1$.
(d) It follows that we can write a_0 as $p_1^{\alpha_1} \cdots p_j^{\alpha_j}$ where the $\alpha_i > 0$ (this is just the prime factorization of a_0). Let $N = a_0 \cdot p_1 \cdot p_2 \cdots p_k$. Show that a_0 divides $f(N)$. Do any of the p_i divide $\frac{f(N)}{a_0}$? What can we conclude if $\frac{f(N)}{a_0} \neq 1$?
(e) Use the fact that every polynomial has a finite number of roots to conclude that $\frac{f(a_0^i N)}{a_0} \neq 1$ for some natural number i. Show that this contradicts our original assumption that only finitely many primes divide $f(n)$ for some natural number n.
(f) Write up the entire proof from beginning to end.

The last problem showed that any non-constant polynomial is divisible by infinitely many primes. This next problem will show that no prime larger than the degree of the polynomial divides the polynomial at every value unless it divides all of the coefficients.

Let p be a prime and $F_p = \{0, 1, ..., p-1\}$ be the remainders modulo p. Recall that every integer has a unique representative in F_p. For example, if p is 2, then every even number is represented by 0 and every odd number is represented by 1. Moreover, we can multiply and add elements of F_p by doing so as we would for integers and then reducing at the end. For example, in F_2, we have $1 + 1 = 0$ since 2 is represented by 0.

Definition 1. A polynomial $f(x)$ with integer coefficients is said to be *over the field F_p* if it is viewed as outputting elements of F_p.

For example if $p = 3$, then the polynomial $5x^2 + 2x - 4$ is the same as $2x^2 + 2x + 2$ when viewed over F_p. This is because $5x^2 + 2x - 4 = 2x^2 + 2x + 2 + 3x^2 - 6 \equiv 2x^2 + 2x + 2 \bmod 3$.

Problem 7. Let p be a prime and f be a non-constant polynomial over F_p of degree $k < p$.

(a) We say that a is a root of f if $f(a) \equiv 0 \bmod p$. Also, we say that a polynomial g divides f if there exists a polynomial h such that $g(x)h(x) = f(x)$. Show that if a is a root of f, then $x - a$ divides $f(x)$. What can you say about the degree of $\frac{f(x)}{x-a}$? (Hint: Remember how this works over the real numbers.)

(b) Use part (a) to show that a non-constant polynomial of degree k over F_p has at most k roots.

(c) Let $f(x)$ now be a non-constant polynomial of degree k with integer coefficients (*not over* F_p). Show that no prime number greater than k can divide $f(n)$ for every natural number n unless that prime divides all the coefficients. (Hint: Reduce modulo p.)

Extra, Extra, Read All About It: A Large Class of Dirichlet's Theorem

In this section, we will prove that Dirichlet's Theorem holds for any a and $b = 1$. (Thank goodness...I have been wondering about this case all day). First, however, we will need to introduce the idea of a cyclotomic polynomial.

Definition 2. We know that $x^n - 1$ has n distinct roots, $\left\{e^{\frac{2\pi ik}{n}}\right\}_{k=0}^{n-1}$, over the complex numbers. The *nth cyclotomic polynomial* $\Phi_n(x)$ is the product of all $\left(x - e^{\frac{2\pi ik}{n}}\right)$ where k and n are relatively prime. Note that $\Phi_n(x)$ is monic or, in other words, has leading coefficient 1 for all n.

Problem 8. Show that $x^n - 1 = \prod_{d|n} \Phi_d(x)$.

Problem 9. (a) Find $\Phi_4(x)$.

(b) Find $\Phi_6(x)$.

(c) Find $\Phi_p(x)$ for p prime.

Problem 10. (a) Prove by induction that $\Phi_n(x)$ has integer coefficients for each n.

(b) Show that the constant term of $\Phi_n(x)$ is ± 1 for all n.

Definition 3. Let $f(x) = a_n x^n + a_{n-1}x^{n-1} \cdots + a_1 x + a_0$ be a polynomial with integer coefficients. We mimic the power rule in defining the *formal derivative* of f as $f'(x) = na_n x^{n-1} + (n-1)a_{n-1}x^{n-2} \cdots + a_1$. The formal derivative is a purely algebraic definition, but it satisfies the typical rules of the differentiation.

Problem 11. Show that if a polynomial f has a multiple root c, then f' will have c as a root.

Problem 12. We are now ready to prove the main result of the section. This will require background in modular arithmetic and group theory.

(a) Show that $\Phi_n(x)$ is greater than 1 for large enough x.

(b) Let p be a prime that does not divide n. Let $m|n$ with $m \neq n$. Prove that $\Phi_n(x)$ and $x^m - 1$ do not have a common root modulo p. (Hint: Use Problem 11.)

(c) Fermat's Little Theorem states that $N^{p-1} \equiv 1 \pmod{p}$ for any N. Let k be the smallest integer for which $N^k \equiv 1 \pmod{p}$. We have proven in other worksheets that k must divide $p - 1$. Using these facts, prove that there are infinitely many primes of the form $an + 1$ for any a.

Definition 4. An integer coefficient polynomial $h(x)$ is *Euclidean* for b modulo a if the prime factors of $h(N)$ for integers N are either congruent to 1 or b modulo a with finitely many exceptions.

Problem 13. Identify the relevant Euclidean polynomials from Problems 3 and 12.

We see that many cases of Dirichlet's Theorem can be proven using Euclidean polynomials. (Yeah I'm pretty sure that's the only way to go with these problems.) Interestingly, not all cases of Dirichlet's Theorem can be proven using Euclidean polynomials. (Okay never mind.) Proving the following results is well beyond the scope of this worksheet, but they are extremely intriguing.

Theorem 2. [Schur, 1912] If $b^2 \equiv 1 \pmod{a}$, then a Euclidean polynomial exists for b modulo a.

Theorem 3. [Murty, 1988] If a Euclidean polynomial exists for b modulo a, then $b^2 \equiv 1 \pmod{a}$.

Problem 14. Find the values of b for which Euclidean polynomials exist modulo 5. Come up with the corresponding Euclidean polynomials.