PRIME GENERATING FUNCTIONS

OLGA RADKO MATH CIRCLE
ADVANCED 2
NOVEMBER 1, 2020

Introduction

The prime numbers underlie much of early and advanced mathematics. Thus it is natural 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 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 functions.

Polynomial Prime Generating Functions that Won't End up Helping Much

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 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. Note you need to show that f cannot output the skipped prime later.
(d) Show that $f(40)$ is not prime without computing the actual output. (Hint: We can write $f(n) = n(n+1) + 41$.)

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. 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.

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.

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 $b = 3$. (Hint: Assume, for the sake of contradiction, that there are finitely many primes of the form $4n + 3$. Construct a number of the form $4n + 3$ that is not divisible by any of the primes of the form $4n + 3$.)

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. (Hint: Recall that prime numbers are 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 of the polynomial be relatively prime. 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.

Since it is difficult to say when polynomials generate infinitely many primes, we can 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, $a_0 = p_1^{\alpha_1} \cdots p_k^{\alpha_k}$. (Hint: What is $f(0)$?)
(c) Show that $a_0 \neq 1$. (Hint: Pick a clever input m, and look at $f(m)$ mod p_i for each $1 \leq i \leq k$.)
(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.

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: Recall that for polynomials

$f(x)$ and $g(x)$ over the integers with $\deg(f) \geq \deg(g)$, there exist polynomials $h(x), r(x)$ such that $\deg(r) < \deg(g)$ and $f(x) = g(x)h(x) + r(x)$. If $g(x) = x - a$ and a is a root of f, what is $r(x)$ mod p?)

(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 mod p and use part (b) to draw a contradiction.)