Prime Generating Polynomials

ANAND PRAKASH

Is there some polynomial $f(z)$ in a variable z, with integer coefficients, that always generates prime numbers, for all possible non-negative integers z? The answer is **No**, and this has been known for long; no such polynomial exists. (See the addendum for a proof.)

However, mathematics enthusiasts from time to time have sought polynomials which generate prime numbers for many consecutive positive integers.

For example, **Leonard Euler** found the quadratic polynomial $f(z) = z^2 + z + 41$ which generates primes for 40 consecutive numbers, namely $z = 0, 1, 2, \ldots, 38, 39$. (It also generates primes for $z = -40, -39, \ldots, -2, -1$, but these primes are identical to the primes generated earlier, because $f(-z-1) = f(z)$, identically.) Other mathematicians have found more examples of such low degree polynomials which display a similar behaviour.

In this article, we play with this theme and offer a few variations of such polynomials.

- Euler's polynomial is of the kind $f(z) = z^2 + z + p$, where p is a prime number. We noted above that it assumes prime values for all z in the set $\{0, 1, 2, \ldots, p-2\}$. There are other polynomials of the same 'shape' that share the same property, for example:

  $f(z) = z^2 + z + 3$: prime for $z \in \{0, 1\}$;

  $f(z) = z^2 + z + 5$: prime for $z \in \{0, 1, 2, 3\}$;

Keywords: Prime number, polynomial, integer coefficient

$f(z) = z^2 + z + 11$: prime for $z \in \{0, 1, 2, \ldots, 8, 9\}$;

$f(z) = z^2 + z + 17$: prime for $z \in \{0, 1, 2, \ldots, 14, 15\}$. (This example was given by the French mathematician **Adrien-Marie Legendre**.)

There do not appear to be any more polynomials of this kind. In other words, it appears that the only values of p for which the polynomial $f(z) = z^2 + z + p$ takes prime values for all $z \in \{0, 1, 2, \ldots, p - 2\}$ are the following: $\{2, 3, 5, 11, 17, 41\}$.

Note that for each of these polynomials, the list of consecutive values of z for which it takes prime values cannot be extended beyond $z = p - 2$, for $z^2 + z + p$ is composite for $z = p - 1$ (and for $z = p$ as well).

- As noted above, Legendre gave the polynomial $f(z) = z^2 + z + 17$ which is prime for all $z \in \{0, 1, 2, \ldots, 14, 15\}$. Closely resembling this are the following:

  $f(z) = z^2 + 3z + 19$: prime for $z \in \{0, 1, 2, \ldots, 13, 14\}$;

  $f(z) = z^2 + 5z + 23$: prime for $z \in \{0, 1, 2, \ldots, 12, 13\}$;

  $f(z) = z^2 + 7z + 29$: prime for $z \in \{0, 1, 2, \ldots, 11, 12\}$.

- Legendre also gave the polynomial $f(z) = 2z^2 + 29$ which is prime for $z \in \{0, 1, 2, \ldots, 27, 28\}$. Closely resembling this are the following:

  $f(z) = 8z^2 + 29$: prime for $z \in \{0, 1, 2, \ldots, 13, 14\}$;

  $f(z) = 10z^2 + 13$: prime for $z \in \{0, 1, 2, \ldots, 11, 12\}$;

  $f(z) = 10z^2 + 7$: prime for $z \in \{0, 1, 2, \ldots, 5, 6\}$;

  $f(z) = 10z^2 + 19$: prime for $z \in \{0, 1, 2, \ldots, 17, 18\}$;

  $f(z) = 12z^2 + 59$: prime for $z \in \{0, 1, 2, \ldots, 13, 14\}$.

- Here are some polynomials that closely resemble Euler's polynomial $z^2 + z + 41$ but differ in the coefficient of z:

  $z^2 + 3z + 43$: prime for $z \in \{0, 1, 2, \ldots, 37, 38\}$;

  $z^2 + 5z + 47$: prime for $z \in \{0, 1, 2, \ldots, 36, 37\}$;

  $z^2 + 7z + 53$: prime for $z \in \{0, 1, 2, \ldots, 35, 36\}$.

  Each of these generates prime values for a relatively long stretch of consecutive values of z.

- Here is an example given by Fung and Ruby: $f(z) = 36z^2 - 810z + 2753$. It takes prime values for $z \in \{0, 1, 2, \ldots, 43, 44\}$. Closely resembling this are the following:

  $f(z) = 36z^2 - 828z + 4363$: prime for $z \in \{0, 1, 2, \ldots, 24, 25\}$;

  $f(z) = 36z^2 - 960z + 7993$: prime for $z \in \{0, 1, 2, \ldots, 14, 15\}$.

- Similar to the above is another example by Fung and Ruby: $f(z) = 47z^2 - 1701z + 10181$. It takes prime values for $z \in \{0, 1, 2, \ldots, 41, 42\}$. Closely resembling this are the following:

  $f(z) = 47z^2 - 1591z + 9631$: prime for $z \in \{0, 1, 2, \ldots, 10, 11\}$;

  $f(z) = 47z^2 - 371z + 8761$: prime for $z \in \{0, 1, 2, \ldots, 9, 10\}$;

  $f(z) = 47z^2 - 901z + 9151$: prime for $z \in \{0, 1, 2, \ldots, 7, 8\}$;

  $f(z) = 67z^2 - 1261z + 9491$: prime for $z \in \{0, 1, 2, \ldots, 7, 8\}$;

  $f(z) = 67z^2 - 561z + 9241$: prime for $z \in \{0, 1, 2, \ldots, 11, 12\}$.

- Lastly, we have this cubic polynomial given by SM Ruiz: $3z^3 - 183z^2 + 3381z - 18757$. It takes prime values for $z \in \{0, 1, 2, \ldots, 41, 42\}$. Closely resembling this are the following:

  $f(z) = 3z^3 - 183z^2 + 3138z - 13487$: prime for $z \in \{0, 1, 2, \ldots, 6, 7\}$;

  $f(z) = 3z^3 - 183z^2 + 2148z - 15277$: prime for $z \in \{0, 1, 2, \ldots, 8, 9\}$.

In this way, we can explore variations in prime generating polynomials which generate prime values for long stretches of consecutive values of the argument. Readers may find more such examples.

References

1. Ed Pegg Jr., "Prime Generating Polynomials", from https://www.mathpuzzle.com/MAA/48-Prime%20Generating%20Polynomials/mathgames_07_17_06.html
2. Weisstein, Eric W. "Prime-Generating Polynomial." From MathWorld–A Wolfram Web Resource. https://mathworld.wolfram.com/Prime-GeneratingPolynomial.html

---

Addendum: A note from the editor

Theorem. It is not possible for a non-constant single-variable polynomial with integer coefficients to take only prime values.

The word 'non-constant' is needed to avoid trivial cases. For example, suppose $f(x) = 2$ for all positive integers x (so it is a constant function); this clearly takes only prime values!

To prove the theorem stated above, we need the two lemmas given below.

Lemma 1. *If $f(x)$ is a polynomial with integer coefficients, then $a - b$ is a divisor of $f(a) - f(b)$ for any two unequal integers a, b.*

To see why this is true, observe first that $a - b$ is a divisor of $a^k - b^k$ for any positive integer k. (The reader should be able to verify this using the factor theorem.) Next, observe that if

$$f(x) = a_n x^n + a_{n-1} x^{n-1} + \cdots + a_1 x + a_0,$$

where $a_0, a_1, \ldots, a_{n-1}, a_n$ are integers, then

$$f(a) - f(b) = a_n (a^n - b^n) + a_{n-1} \left(a^{n-1} - b^{n-1}\right) + \cdots + a_1 (a - b).$$

Since $a - b$ is a divisor of each bracketed term on the right, it follows that $a - b$ is a divisor of $f(a) - f(b)$.

Lemma 2. *If $f(x)$ is a polynomial with positive leading coefficient, then if x is sufficiently large, $f(x)$ is positive and strictly increasing. (In short, any polynomial function with positive leading coefficient ultimately becomes "positive and strictly increasing.")*

Outline of proof:

- Since $f(x)$ is a polynomial with positive leading coefficient, this is also true for $f'(x)$. That is, the derivative is a polynomial with positive leading coefficient.
- It follows that the derivative will be positive for large enough x, because the leading term in $f'(x)$, which will dominate all terms with lower degree for large enough x, will be positive.
- Since $f'(x)$ is positive for large enough x, $f(x)$ is strictly increasing for large enough x.
- Since $f(x)$ has integer coefficients, it is integer-valued. Therefore, when x increases from any integer to the next higher integer, $f(x)$ increases by ≥ 1. Hence $f(x)$ assumes positive values for large enough x. (More can be said: $f(x)$ grows without bound.)

Proof of the main claim. Let $f(x)$ be a non-constant polynomial with integer coefficients, with positive leading coefficient. To show that $f(x)$ cannot take only prime values, we only need to exhibit a single composite value taken by f. We shall exhibit such a value.

Suppose that for $x \geq N$, $f(x)$ is increasing, and $f(x) > 1$. Let $f(N) = q$. Then $q > 1$. Now consider the number

$$f(N+q) - f(N).$$

Invoking Lemma 1, we infer that $f(N+q) - f(N) = f(N+q) - q$ is divisible by q. Since $f(N) = q$, this implies that $f(N+q)$ too is divisible by q. Also, $f(N+q) > q$, since $f(N+q) > f(N)$. This implies that $f(N+q)$ is composite. We have thus succeeded in exhibiting a composite value taken by $f(x)$. □

ANAND PRAKASH runs a small garment shop at Kesariya village in the state of Bihar. He has a keen interest in number theory and recreational mathematics and has published many papers in international journals in these fields. He also has a deep interest in classical Indian music as well as cooking. In addition, he has written a large number of poems in Hindi. He may be contacted at prakashanand805@gmail.com.