Euler's prime-generating polynomial

Arjen Markus

August 25, 2023

Introduction

The polynomial $P(x) = x^2 + x + 41$ has the remarkable property that its values are all prime for $x = 0...39$. You can of course also fill in negative values of x, but these give the same primes.

The first 50 values are shown in the table below:

Table 1: First 50 numbers generated by Euler's polynomial

x	0	1	2	3	4	5	6	7	8	9
P(x)	41	43	47	53	61	71	83	97	113	131
x	10	11	12	13	14	15	16	17	18	19
P(x)	151	173	197	223	251	281	313	347	383	421
x	20	21	22	23	24	25	26	27	28	29
P(x)	461	503	547	593	641	691	743	797	853	911
x	30	31	32	33	34	35	36	37	38	39
P(x)	971	1033	1097	1163	1231	1301	1373	1447	1523	1601
x	40	41	42	43	44	45	46	47	48	49
P(x)	1681	1763	1847	1933	2021	2111	2203	2297	2393	2491
	=41*41	=41*43			=43*47					=47*53

At $x = 40$, this breaks down:

$$40^2 + 40 + 41 \quad = \quad 40 \cdot (40 + 1) + 41 = 41 \cdot 41 = 1681 \tag{1}$$

Filling in $x = 41$ gives: $P(41) = 1763 = 43 \cdot 41$ – again a factor 41.

The polynomial is known as Euler's prime-generating polynomial and is the best known example of such polynomials. Other polynomials of the form $P(x) = x^2 + x + p$ (where p is a prime) that also generate primes from $x = 0...p - 2$ exist: the value of p can be 2, 3, 5, 11, 17 and 41.[1]

[1] See for instance `https://mathworld.wolfram.com/Prime-GeneratingPolynomial.html`.

Can you generate more primes?

It is well known that no (simple) polynomial will generate only prime numbers. That can be demonstrated quite simply:

- Consider the number $b = P(a)$ for any polynomial $P(x)$ of degree n, where a is some value, $a = 0$ will do, but $a = 1$ or $a = 123$ as well.
- Now consider the number $x = kb + a$, where $k = 0, 1, ...$ We can find a straightforward expression for the value of $P(x)$ by inserting it in the expression for the polynomial:

$$\begin{aligned} P(x) &= P(kb + a) \\ &= A \cdot (kb + a)^n + B \cdot (kb + a)^{n-1} + ... + Y \cdot (kb + a) + Z \\ &= A' \cdot (kb)^n + B' \cdot (kb)^{n-1} + ... + Y' \cdot (kb) + A \cdot a^n + B \cdot a^{n-1} + ... + Z \\ &= A' \cdot (kb)^n + B' \cdot (kb)^{n-1} + ... + Y' \cdot (kb) + b \qquad (2) \end{aligned}$$

  (the coefficients $A, B, ...Z$ and $A', B', ... + Y'$ are simply related.)

The essence of equation 2 is that for values of the form $x = k \cdot b + a$, the value $P(x)$ is divisible by $b = P(a)$. Hence: once a particular value occurs in the series $P(0), P(1), P(2), ...$, new values will occur at regular intervals that have this value as one of the factors. And: these factors do not need to be prime.

Other polynomials exist that can generate a few more primes but in the end they all break down in the above manner.[2]

What about the factors?

Now, the next step is to examine the factors of the values $P(x)$ that are generated, whether these values are primes or not. Let us start with a simple observation: all values $P(x)$ are odd. If x is even, then $x^2 + x$ is even as well, so $P(x)$ is odd. If x is odd, then, again, $x^2 + x$ is even and thus $P(x)$ is odd.

If we look at 3 as a possible factor, we need to do a bit more work. Consider the polynomial *modulo 3*:

$$P(x) \equiv x^2 + x + 2 \pmod 3 \qquad (3)$$

We need to consider only $x = 0, 1, 2 \pmod 3$ and then $P(x) = 2, 1, 2 \pmod 3$. Therefore, there are no values $P(x)$ that have a factor 3.

We can continue and find that *there are no factors smaller than 41!*. In fact, the smallest factor that does not occur in table 1 is 163, followed by 167, 179, 199 and 227.

It may seem remarkable that there are no smaller factors than 41 possible and no smaller factors outside the 40 primes than 163. However, we can analyse this in the same way as in the previous section:

[2]The Mathworld page mentions the existence of polynomials with many variables that apparently can generate all primes, but not consecutively.

Express a number x as $x = kp + a$, where p is the prime for which we seek an answer to the question "can it occur as a factor of $P(x)$?", a runs from 0 to $p - 1$ and we take the polynomial as mod p. Then:

$$\begin{aligned} P(x) &\equiv P(kp + a) \\ &\equiv A \cdot (kp + a)^n + B \cdot (kp + a)^{n-1} + ... + Y \cdot (kp + a) + Z \qquad (4) \\ & \qquad (5) \end{aligned}$$

Since we take the expression as mod p, it can be simplified to:

$$\begin{aligned} P(x) &\equiv A \cdot a^n + B \cdot a^{n-1} + ... + Y \cdot a + Z \\ &\equiv P(a) \qquad (6) \end{aligned}$$

We know that $P(a)$ is a prime number equal to or larger than 41, for all values of a from 0 to 39, so no prime p smaller than $39 + 1$ (39 being the maximum value for a in the equation) can occur as a solution for:

$$P(a) \equiv 0 \mod p \qquad (7)$$

The series $P(0), P(1), ...P(39)$ does not contain all primes between 41 ($= P(0)$) and 1601 ($= P(39)$), so there is room for prime factors lower than 1601, like 163 and the others mentioned above. Similar conclusions hold for other polynomials that generate primes, as the line of reasoning above is not specific to Euler's polynomial.