A prime producing polynomial

Observations on the Trinomial $n^2 + n + 41$

By Matt C. Anderson

March 9 2021

In number theory,

We assume that n is an integer. We focus our attention on the polynomial $n^2 + n + 41$. Further, we analyze the behavior of the factorization of integers of the form

$$q(n) = n^2 + n + 41. \qquad \text{(expression 1)}$$

where n is a non-negative integer. It was shown by Legendre, in 1798 that if $0 \leq n \leq 40$ then r(n) is a prime number. Certain patterns become evident when considering points (a,n) where

$$q(n) \equiv 0 \bmod a. \qquad \text{(expression 2)}$$

The collection of all such points produces what we are calling a "graph of discrete divisors". It has certain repeated features. From experimental data, we find that the integer points in this dataset are contained by parabolas. And more, the parabolas are described by a closed form expression. We see that the parabolas are indexed (r,c) by pairs of relatively prime integers. The expression for the middle parabolas is

$$p(r,c) = (c*x - r*y)^2 - x*(c*x - r*y) - x + 41*r^2 \qquad \text{(expression 3)}$$

The restrictions on p(r,c) are that $0<r<c$ and gcd(r,c) = 1. Where gcd() means greatest common divisor of two arguments. And all four of r,c,x, and y are integers.

When we take the derivative of p(r,c) with respect to x and set this expression equal to zero, we obtain

$$x = (163*r^2)/4 \qquad \text{(expression 4)}$$

Each such pair (r,c) yields (again determined experimentally and by observation of calculation in a computer algebra system) an integer polynomial $a*z^2 + b*z + c$. The first few (r,c) pairs are (2,1); (3,2); (3,1); (4,3); (4,1) and (5,4). Again, r and c must be relatively prime numbers. Further, the quartic $r(a*z^2 + b*z + c)$ will factor algebraically over the integers into two quadratic expressions. We call this our "parabola conjecture" (or conjecture 'a'). Certain structure in the 'graph of discrete divisors' are do to elementary relationships between pairs of co-prime integers.

We conjecture that all composite values of r(n) arise by substituting integer values of z into $q(a*z^2 + b*z + c)$, where this quartic divisors algebraically over **Z** for $a*z^2 + b*z + c$ a quadratic polynomial determined by a pair of relatively prime integers (r, c). We are confident of this conjecture because of the structure of the graph of discrete divisors produced by some computer code in our computer algebra system (Maple). We call this our "no stray points conjecture" (or conjecture 'b') because all the points in the graph appear to lie on a parabola.

We further conjecture that the minimum x-values for parabolas corresponding to (r, c) are given by expression 4. The vertical lines $x = 163*c^2/4$ where c = 2, 3, 4, … The numerical evidence seems to support this. This is called our "parabolas line up conjecture.

Theorem 1 – Consider r(n) with n a non negative integer. Then,
r(n) never has a factor less than 41.

We prove Theorem 1 with a modular construction. We make a residue table of r(y) mod x, with all the prime divisors less than 41. A form of the fundamental theorem of arithmetic states that any integer greater than one is either a prime number, or can be written as a unique product of prime numbers (ignoring the order). So if r(n) never has a prime factor less than 41, then by extension it never has a prime factor less than 41.

For example, to determine that r(n) is never divisible by 2, note the first column of the residue table. If n is even then r(n) is odd. Similarly, if n is odd then r(n) is

also odd. In either case, r(n) does not have factorization by 2. Since all integers are either even or odd, r(n) is never divisible by 2 when n is a positive integer.

Also, for divisibility by 3, there are 3 cases to check. They are $n \equiv 0$, 1, and 2 mod 3. r(0) mod 3 is 2. r(1) mod 3 is 1 and r(2) mod 3 is 2. Since none of these results is 0, we have that r(n) is never divisible by 3. This is the second column of the residue table.

The number 0 is first found in the residue table for the cases r(0) mod 41 and r(40) mod 41. We can see that $40^2 + 40 + 41 = 41^2$. This means that if n is congruent to 0 mod 41 then r(n) will be divisible by 41. What's more is that these are the only two cases for divisibility by 41. Similarly, if n is congruent to 40 mod 41 the r(n) will also be divisible by 41.

After the residue table, we observe a curve fit to our 'graph of discrete divisors' which has points when q(y) mod x is divisible by x. This is an exact curve fit. The points (x,y) can be seen in a data table, and on a bifurcation graph.

< see residue table >

Thus we have shown that q(n) never has a factor less than 41.

Theorem 2

Since $q(a) = a^2 + a + 41$, we want to show that q(a) = q(-a-1).

Proof of theorem 2
Because q(a) = a*(a+1) + 41,
Now q(-a -1) = (-a -1)*(-a -1 +1) + 41.
So q(-a -1) = (-a –1)*(-a) + 41,
And q(-a -1) = q(a).
End of proof of theorem 2.

Corrolary 1
Further, if r(b) mod c ≡ 0 then q(c –b -1) mod c ≡ 0.

We see that it is amazing that the data points all fall within an exact curve fit. All the parabolas have integer coefficients.

End