A prime producing polynomial.

Observations on the trinomial $n^2 + n + 41$.

by Matt C. Anderson

August 2016

The story so far

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

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

where n is a non-negative integer. It was shown by Legendre, in 1798 that if $0 \le n < 40$ then h(n) is a prime number.

Certain patterns become evident when considering points (a,n) where

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

The collection of all such point produces what we are calling a "graph of discrete divisors" due to certain self-similar features. From experimental data we find that the integer points in this bifurcation graph lie on a collection of parabolic curves indexed by pairs of relatively prime integers. The expression for the middle parabolas is –

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

The restrictions are that $0<r<c$ and $\gcd(r,c) = 1$ and all four of r,c,x, and y are integers.

Each such pair (r,c) yields (again determined experimentally and by observation of calculations) an integer polynomial a*z2 + b*z + c, and the quartic h(a*z2 + b*z + c) then factors non-trivially over the integers into two quadratic expressions. We call this our "parabola conjecture". Certain symmetries in the bifurcation graph are due to elementary relationships between pairs of co-prime integers. For instance if $m<n$ are co-prime integers, then there is an observable relationship between the parabola it determines that that formed from (n-m, n).

We conjecture that all composite values of h(n) arise by substituting integer values of z into $h(a*z^2 + b*z + c)$, where this quartic factors algebraically over **Z** for $a*z^2 + b*z + c$ a quadratic polynomial determined by a pair of relatively prime integers. We name this our "no stray points conjecture" because all the points in the bifurcation graph appear to lie on a parabola.

We further conjecture that the minimum x-values for parabolas corresponding to (r, c) with gcd(r, c) = 1 are equal for fixed n. Further, these minimum x-values line up at $163*c^2/4$ where c = 2, 3, 4, ... The numerical evidence seems to support this. This is called our "parabolas line up" conjecture.

The notation gcd(r, c) used above is defined here. The greatest common divisor of two integers is the smallest whole number that divides both of those integers.

Theorem 1 - Consider h(n) with n a non negative integer.
h(n) never has a factor less than 41.

We prove Theorem 1 with a modular construction. We make a residue table with all the prime factors less than 41. 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 h(n) never has a prime factor less than 41, then by extension it never has an integer factor less than 41.

For example, to determine that h(n) is never divisible by 2, note the first column of the residue table. If n is even, then h(n) is odd. Similarly, if n is odd then h(n) is also odd. In either case, h(n) does not have factorization by 2.

Also, for divisibility by 3, there are 3 cases to check. They are n = 0, 1, and 2 mod 3. h(0) mod 3 is 2. h(1) mod 3 is 1. and h(2) mod 3 is 2. Due to these three cases, h(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 h(0) mod 41 and h(40) mod 41. This means that if n is congruent to 0 mod 41 then h(n) will be divisible by 41. Similarly, if n is congruent to 40 mod 41 then h(n) is also divisible by 41.
After the residue table, we observe a bifurcation graph which has points when h(y) mod x is divisible by x. The points (x,y) can be seen on the bifurcation graph.

< insert residue table here >

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

Theorem 2

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

Proof of Theorem 2
Because h(a) = a*(a+1) + 41,
Now h(-a -1) = (-a -1)*(-a -1 +1) + 41.
So h(-a -1) = (-a -1)*(-a) +41,
And h(-a -1) = h(a).
Which was what we wanted.
End of proof of theorem 2.

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

We can observe interesting patterns in the “graph of discrete divisors” on a following page.