A prime producing polynomial.

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

by Matt C. Anderson

May 2021

In number theory,

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.

Given that n is restricted to positive integers, it is an unsolved problem whether or not h(n) is a prime number an infinite number of times. I suspect that h(n) is prime infinitely often. Numerical evidence supports this.

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

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

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 devisor of two integers is the smallest whole number that divides both of those integers.

Theorem 1 – The only small factors theorem - 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. Also, we test all possible residues for each prime.

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.

< see residue table in appendix 4 >

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

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.

Theorem 2 – the near mirror symmetry theorem

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

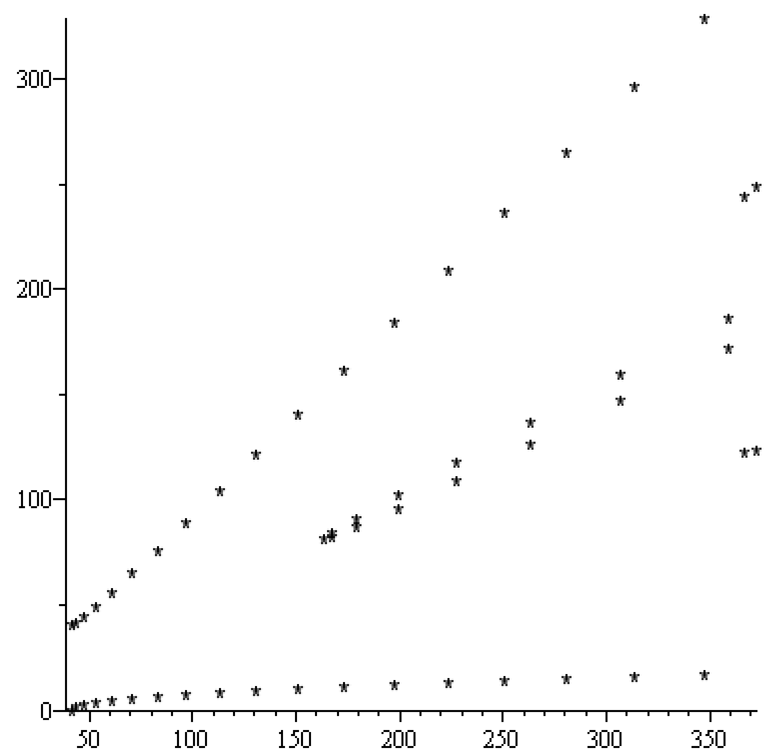
Proof of Theorem 2
Because h(a) = a*(a+1) + 41,

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.

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

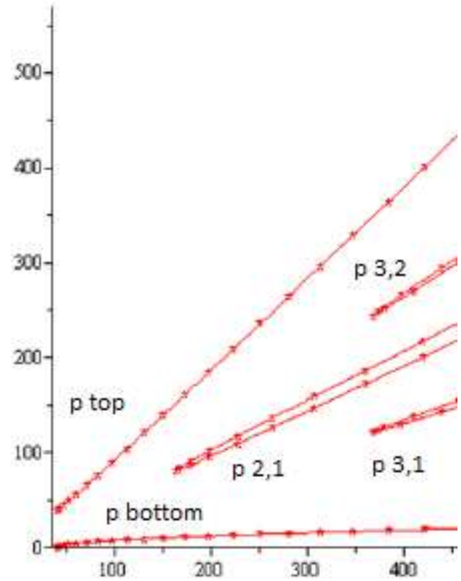
We can observe interesting patterns in the graph of discrete divisors on a following page.

plot(x, y, style = point, symbol = asterisk, color = black)



this is a graph of 55 data points of $y^2 + y + 41$ **mod** $x = 0$.
It can be curve fit with parabolas.
This graph shows 5 parabolas
The names of the parabolas are p_{top}; p_{bottom}; $p_{2,1}$; $p_{3,2}$; **and** $p_{3,1}$.

The curve fit data is shown below.



Graph of discrete divisors.

Undiscovered Expressions

So far, we want to determine when $h(n) = n^2 + n + 41$ is a prime number. We produce a dataset that satisfies the congruency $h(y) \equiv 0 \bmod x$. In other words, we find ordered pairs (x,y) such that x divides h(y). The graph of all pairs (x,y) seems to have obvious regularity and patterns. We are able to tabulate coefficients of parabolas that exactly fit the data. Here are the first few parabolas :

P bottom x (z) = $z^2 + z + 41$
P bottom y (z) = z

P top x (z) = $z^2 - z + 41$
P top y (z) = $z^2 + 40$

P 2,1 x (z) = $4*z^2 + 163$
P 2,1 y (z) = $2*z^2 + z + 81$

P 3,2 x (z) = $4*z^2 + 163$
P 3,2 y(z) = $6*z^2 + z + 244$

P 3,1 x (z) = $z^2 + z + 41$
P 3,1 y (z) = $3*z^2 + 2*z + 122$

A computer tool can show that h(P 2,1 x(z)) = P 2,1 y(z) * ($z^2 + z + 41$). (equation *)

The Maple command subs() can substitute one expression into another. Also the Maple command factor() can factor quartic polynomials.

The important part of equation * is that the right hand side is the product of two integers, both greater than one. This proves that h(P 2,1(z)) is a composite number. In other words, if you put a positive integer of the form $4*z^2 +163$ as input to h(n), then you will get a composite number as output.

We have the general parabola

P c,r x(z) and P c,r y(z).

I was unable to determine these expressions. It may be impossible and it is related to the distribution of prime numbers.

My naming scheme for the parabolas requires c and r to be integers and

0>r>c and gcd(r,c) = 1

Where gcd is the Greatest Common Divisor of two integers.

So the first few parabolas are, besides top and bottom,

P 2,1

P 3,1	P 3,2		
P 4,1		P 4,3	
P 5,1	P 5,2	P 5,3	P 5,4

Hopefully the naming convention for P c,r is now clear.

I was able to determine an expression for P c,r that eliminates z.

This is expression 3 from before

$P\ r,c = (c*x - r*y)^2 - r*(c*x - r*y) - x + 41*r^2$

We assume r and c are integers.

Appendix 1 - Maple Code for graph of discrete divisors

```
x := Vector(55) :
y := Vector(55) :
counter := 1 :
for a from 2 to 378 do
for b from 0 to a − 1 do
if mod(b^2 + b + 41, a) = 0
  then x[counter] := a : y[counter] := b : counter := counter + 1;
end if;
end do:
end do:
```

The number 378 was chosen by trial and error to completely fill the vector of length 55. The number 55 was chosen so that we can easily identify 5 parabolas from the data points.

This code creates a data set and stores it in two vectors.

Appendix 2 – Mape Code for exact curve fit parabolas

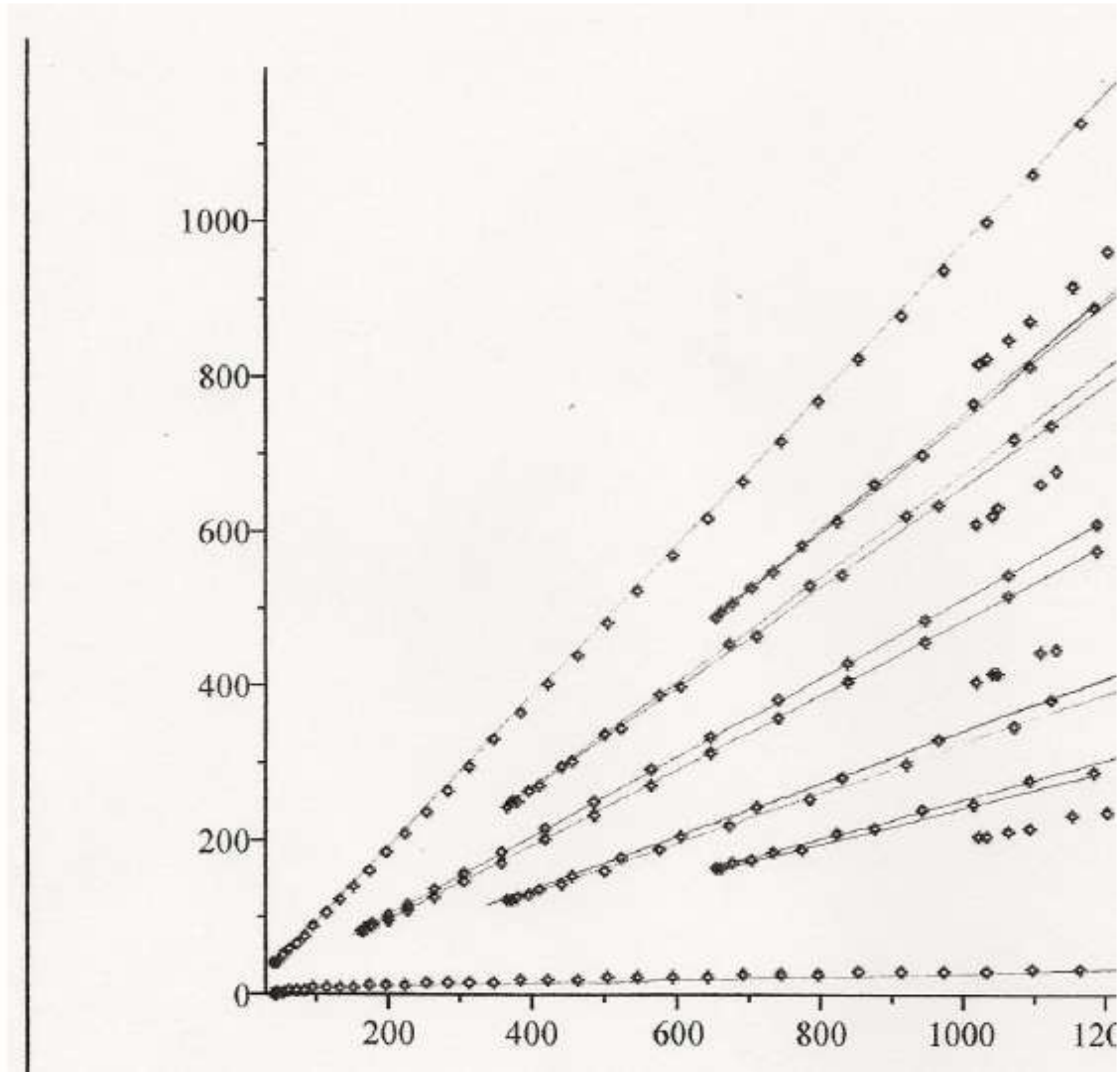
```
> x[1, 1, bottom] := z^2+z+41; y[1, 1] := z;
> p2 := plot([x[1, 1, bottom], y[1, 1], z = 0 .. 20]);
> with(plots);
> display(p2);
>
> x[1, 1, top] := z^2+z+41; y[1, 1, top] := z^2+40;
> p3 := plot([x[1, 1, top], y[1, 1, top], z = 0 .. 20]);
> display(p3);
>
> y[2, 1] := 2*z^2+z+81; x[2, 1] := 4*z^2+163;
> p4 := plot([x[2, 1], y[2, 1], z = -10 .. 10]);
> display(p4);
>
> y[3, 1] := 3*z^2+2*z+122; x[3, 1] := 9*z^2+3*z+367;
> p5 := plot([x[3, 1], y[3, 1], z = -4 .. 3]);
>
> y[3, 2] := 6*z^2+z+244; x[3, 2] := 9*z^2+3*z+367;
> p6 := plot([x[3, 2], y[3, 2], z = -4 .. 3]);
```

This code shows that parabolas exactly fit the data produced by (expression 2).

See graph above.

Appendix 3

Graph of discrete divisors with 7 parabolas.



The data in this graph seems to appear with a (mostly) regular pattern.

Appendix 4 – residue table

Residue Table

	2	3	5	7	11	13	17	19	23	29	31	37	41	43
0	1	2	1	6	8	2	7	3	18	12	10	4	0	41
1	1	1	3	1	10	4	9	5	20	14	12	6	2	0
2		2	2	5	3	8	13	9	1	18	16	10	6	4
3			3	4	9	1	2	15	7	24	22	16	12	10
4			1	5	6	9	10	4	15	3	30	24	20	18
5				1	5	6	3	14	2	13	9	34	30	28
6				6	6	5	15	7	14	25	21	9	1	40
7					9	6	12	2	5	10	4	23	15	11
8					3	9	11	18	21	26	20	2	31	27
9					10	1	12	17	16	15	7	20	8	2
10					8	8	15	18	13	6	27	3	28	22
11						4	3	2	12	28	18	25	9	1
12						2	10	7	13	23	11	12	33	25
13							2	14	16	20	6	1	18	8
14							13	4	21	19	3	29	5	36
15							9	15	5	20	2	22	35	23
16							7	9	14	23	3	17	26	12
17								5	2	28	6	14	19	3
18								3	15	6	11	13	14	39
19									7	15	18	14	11	34
20									1	26	27	17	10	31
21									20	10	7	22	11	30
22									18	25	20	29	14	31
23										13	4	1	19	34
24										3	21	12	26	39
25										24	9	25	35	3
26										18	30	3	5	12
27										14	22	20	18	23
28										12	16	2	33	36
29											12	23	9	8
30											10	9	28	25
31												34	8	1
32												24	31	22
33												16	15	2
34												10	1	27
35												6	30	11
36												4	20	40
37													12	28
38													6	18
39													2	10
40													0	4
41														0
42														41

Explaination of Residue Table
column index, C are across the top
row index, R are found along the side

table values are calculated by
R^2 + R + 41 mod C

Notice that columns
with 41 and 43 contain 0 twice.

These 0 values become points in the
graph of discrete divisors.

Thus we have tried all prime divisors from 2 to 37 inclusive. None of them give a zero residue. The four residues in the residue table involve divisibility by 41 and 43.