A prime producing quadratic expression

By Matthew Anderson
April, 2016
ORMATYC conference
Salishan Oregon

An interesting quadratic expression

- $h(x) = x^2 + x + 41$

Is prime for x= 0 .. 39

Never has a divisor less than 41

Has an interesting pattern of being prime or composite

In this presentation expect two proofs – one by logical inference, one by trying all possibilities.

Warm up exercise
Quadratic Expressions that factor

Let $f(x) = x^2 - 5x + 6$ and x be an integer.

What do we do with trinomials like this?

We factor them.

Warm up exercise
Quadratic Expressions that factor

Let $f(x) = x^2 - 5x + 6$ and x be an integer.

Warm up exercise
Quadratic Expressions that factor

Let $f(x) = x^2 - 5x + 6$ and x be an integer.

$f(x) = (x-2)(x-3)$

If f(x) is prime, one of the terms must be equal to ± 1.

There will be 4 cases.

For primality, require $x-2 = \pm 1$ or $x-3 = \pm 1$.

So the 4 cases are x = 1,3 ; 2, 4

Warm up exercise
Quadratic Expressions that factor

Let $f(x) = x^2 - 5x + 6$ and x be an integer.

$f(x) = (x-2)(x-3)$

If f(x) is prime, one of the terms must be equal to ± 1.

There will be 4 cases.

For primality, require $x-2 = \pm 1$ or $x-3 = \pm 1$.

So the 4 cases are x = 1,3 ; 2, 4

x	f(x)
0	6
1	2
2	0
3	0
4	2
5	6
6	12

Warm up exercise
Quadratic Expressions that factor

Let $f(x) = x^2 - 5x + 6$ and x be an integer.

$f(x) = (x-2)(x-3)$

If f(x) is prime, one of the terms must be equal to ± 1.

There will be 4 cases.

For primality, require $x-2 = \pm 1$ or $x-3 = \pm 1$.

So the 4 cases are x = 1,3 ; 2, 4

x	f(x)
0	6
1	2
2	0
3	0
4	2

Any quadratic function that factors linearly in the integers and has integer input will be prime for at most 4 input values. (There is a proof around here somewhere ☺)

Theorem 1 Any quadratic function that factors linearly in the integers and has integer input will be prime for at most 4 input values.

Proof

Let f(x) be a trinomial. Explicitly $f(x) = (x-a)*(x-b)$.

We want f(x) a prime number with x an integer.

Set both parts equal to ±1.

Then $x-a = \pm 1$ and $x-b = \pm 1$.

It follows that

$x = b \pm 1$ and $x = a \pm 1$.

These are the only possibilities for a prime number f(x).

Which was what we wanted.

pause

First few values of h(x)

x	h(x)
0	41
1	43
2	47
…	
39	1601

By inspecting the table, we can deduce that x^2+x+41 is prime for $0 \le x \le 40$

note that $h(x) = x(x+1) + 41$.

so $h(40) = 40*41 + 41 = 41^2$.

Divisibility by 2

- $h(x) = x^2 + x + 41$
- The square of an even number is even.
- The square of an odd number is odd.
- The sum of 2 even numbers and an odd is odd.
- The sum of 3 odd numbers is odd.
- $h(x)$ is always odd, no matter if x is even or odd.
- $h(x)$ is never divisible by 2.

Divisibility by 3

Again $h(x) = x^2 + x + 41$.

There are 3 possible remainders mod 3.

0, 1, and 2

$h(0) \bmod 3 = 2$

$h(1) \bmod 3 = 1$

$h(2) \bmod 3 = 2$

Since $h(x) \bmod 3$ is never 0,

$h(x)$ is never divisible by 3.

Prime Divisors less than 41

I built an excel table. The rows are the remainders and the columns are the primes. Each entry at location (r,c) is evaluated as

$(r^2 + r + 41) \bmod c$

If the value is 0 then $h(x)$ is divisible by c, as long as $x = r \bmod c$.

Residue table

If x= 0 mod 41 or 40 mod 41 then h(x) is divisible by 41. Also, If x= 1 or 41 mod 43 then 43 divides h(x). Either way, h(x) is composite.

Since there are no zero values in the table for primes smaller than 41, h(x) is never divisible by any prime smaller than 41.

	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											10	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**

A theorem about h(n)

Let h(a) = a*(a+1) + 41.

Show that h(a) = h(-a -1).

Proof   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) = (a + 1)*a + 41.

Thus h(-a -1) = h(a).

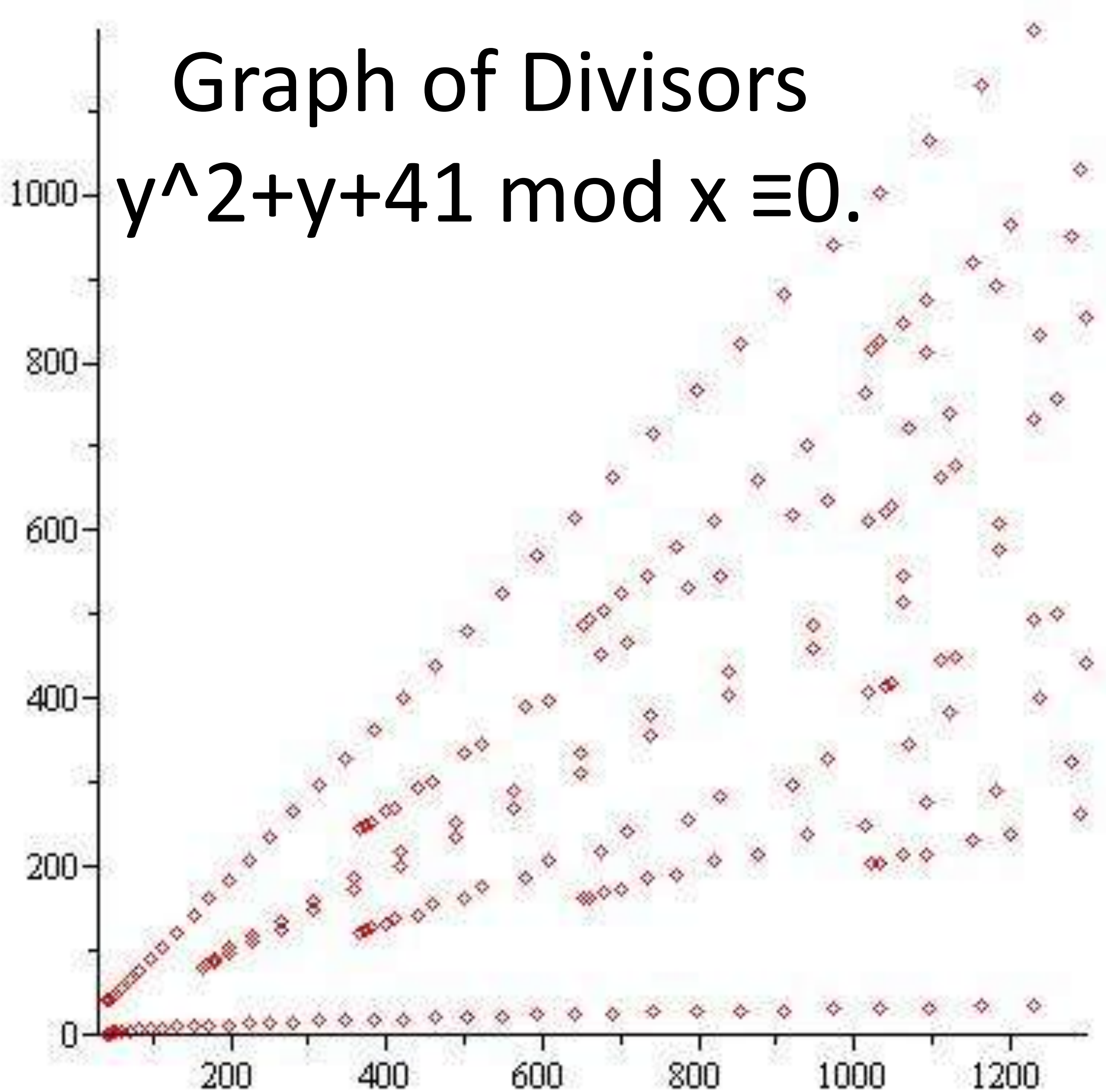
Which was what we wanted.

From a lookup table to a graph

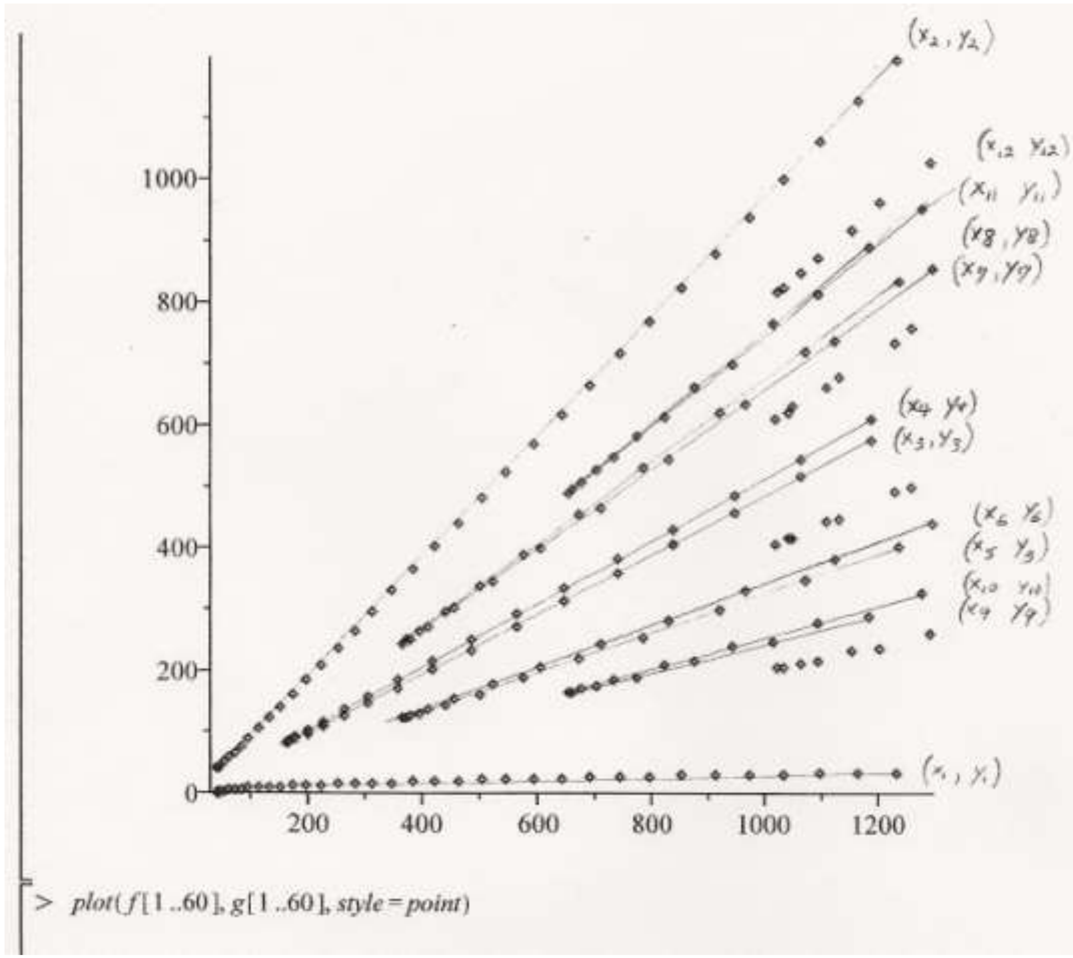
- The x axis is the integers. I did not just use the primes, because allowing for composite divisors makes the patterns easier to see.
- The y axis are the same as in the table.
- If h(y) mod x = 0 then plot a point.
- Every time h(x) is composite, there is at least one corresponding point on the graph.

Graph of Divisors

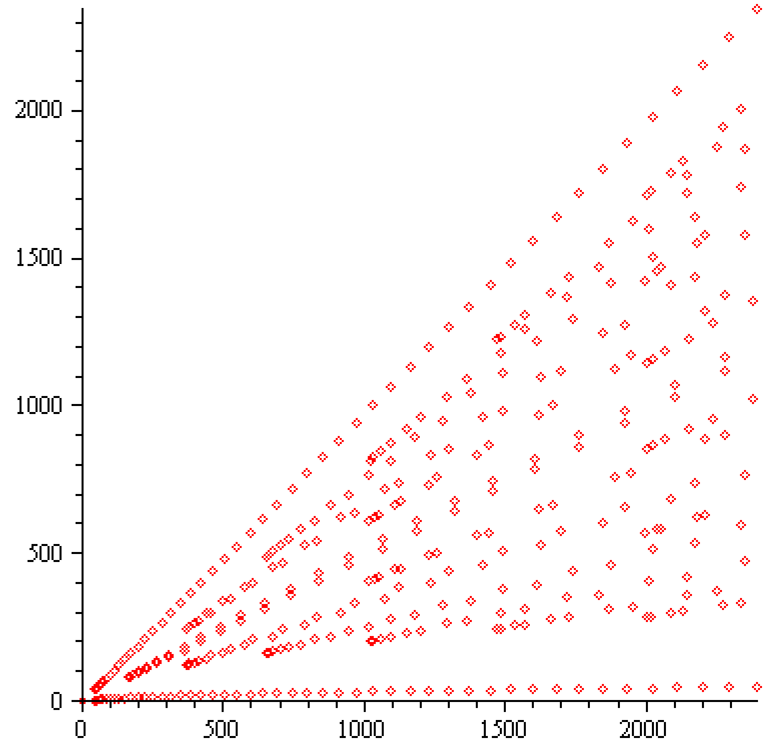
y^2+y+41 mod x ≡0.



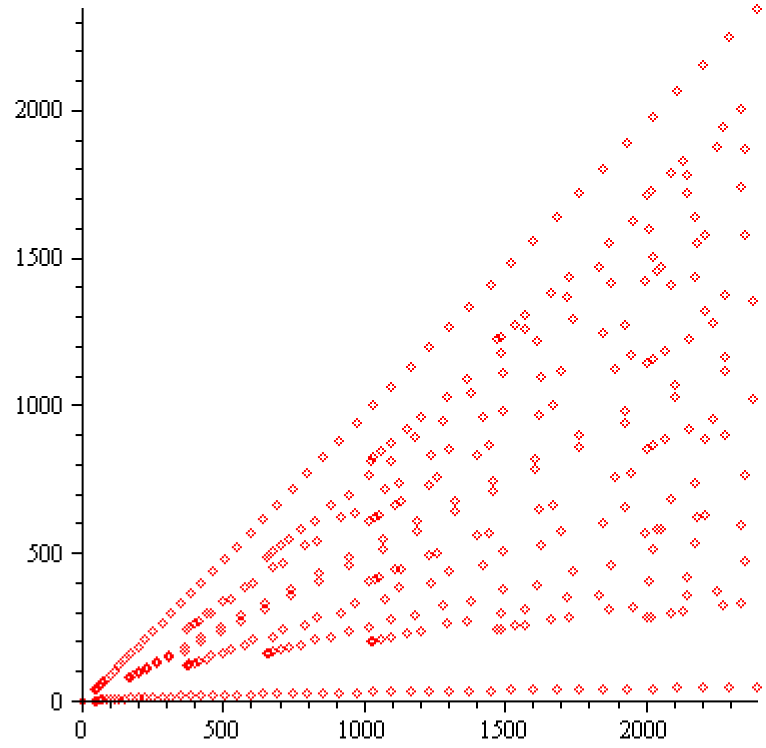
Patterns in the graph of divisors



Count the parabolas by columns

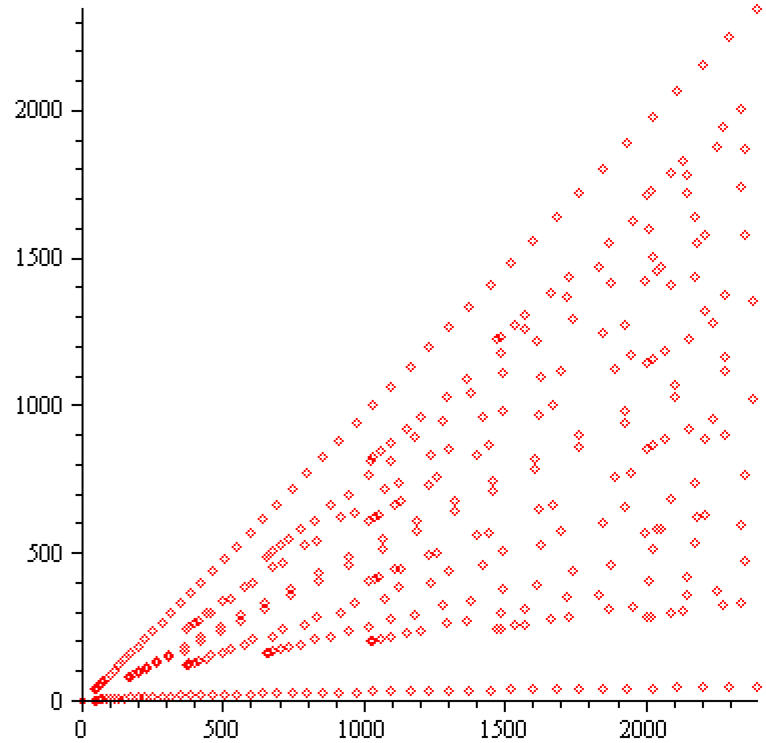


Count the parabolas by columns



1, 1, 2, 2, 4, 2, 6

Count the parabolas by columns



1, 1, 2, 2, 4, 2, 6

The Euler phi function exactly describes this sequence.
oeis.org/A10

Numbering scheme for parabolas

Let r stand for row

Similarly let c stand for column

Let p(r,c) be the parabola indexed by r , c.

Require that $0<c<r$

Also Require that

$\mathrm{Gcd}(r,c) = 1$.

That is, the row and column index must be relatively prime.

Describe equations for parabolas

- For example, if $y_{2,1}(x) = x^2 + 40$ then the composition of functions h(g(x)) factors algebraically.
- $h(x) = x^2 + x + 41$
- $h(y(x)) = (x^2+40)^2 + (x^2+40) + 41$
- $Hoy(x) = (x^2+x+41)(x^2-x+41)$

This is a 4th order polynomial with algebraic factorization.

Two more one parameter expressions

Use the technique of composition of functions

- Y[3,1] = 2*z^2 + z + 81
  x[3,1] = h(y[3,1](z))

X[3,1] = (4z^2+ 163)*(z^2 + z + 41)

Y[3,2] = 3*z^2 + 2*z + 122
  x[3,2] = (9*z^2 + 3z + 367)*(z^2 + z + 41)

Data for the graph

- Values (y,x) that make h(x) divisible by y
- And h(x) is still x^2 + x + 41

(41,0)

(41,40)

(43,1)

(43,41)

(47,2)

Note that if x=41*k then h(x) = 41*{41k^2+k+1}

This would make h(x) composite.

A 2 parameter expression

$h(n) = n^2 + n + 41$

$y(a,z) = a*z^2 + (a-1)*z + 41*a - 1$

Through the composition of functions

$h(y(a,z)) = (z^2+z+41) *$

$(a^2*z^2+z*a^2-a+41*a^2+1)$

Again, this algebraic factorization indicates that $h(n)$ is composite for all integers a and z.

Conjecture

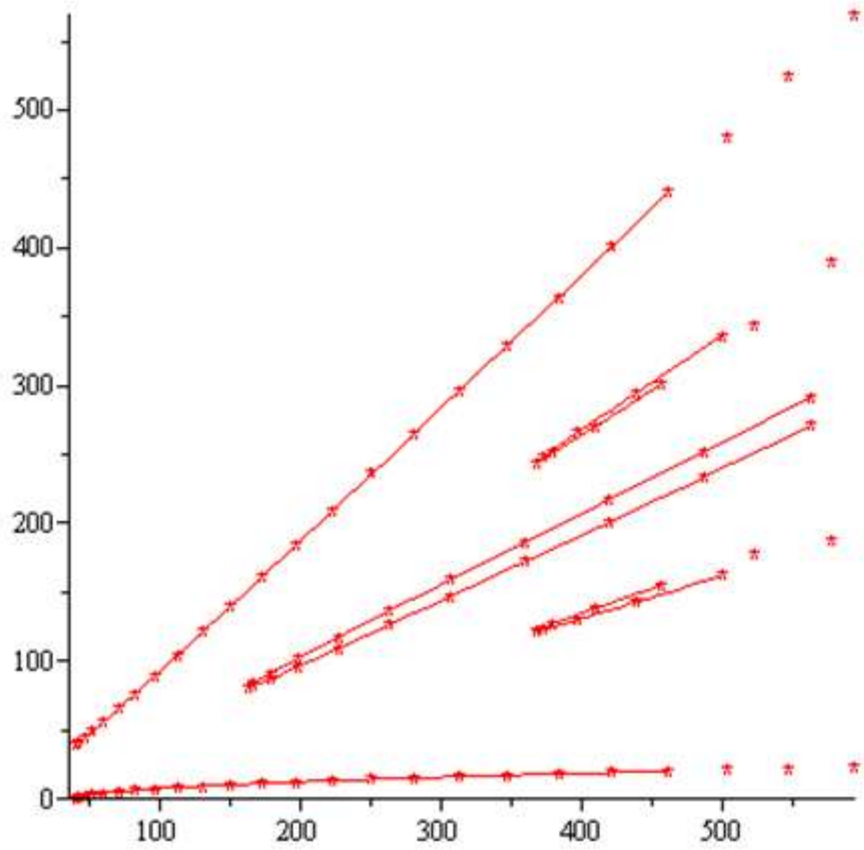
I conjecture that there is an expression in many variables that restricts n and completely covers all the cases that h(n) is composite.

If this was true, one could possibly prove that h(n) is prime an infinite number of times.

Maple 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]);
```

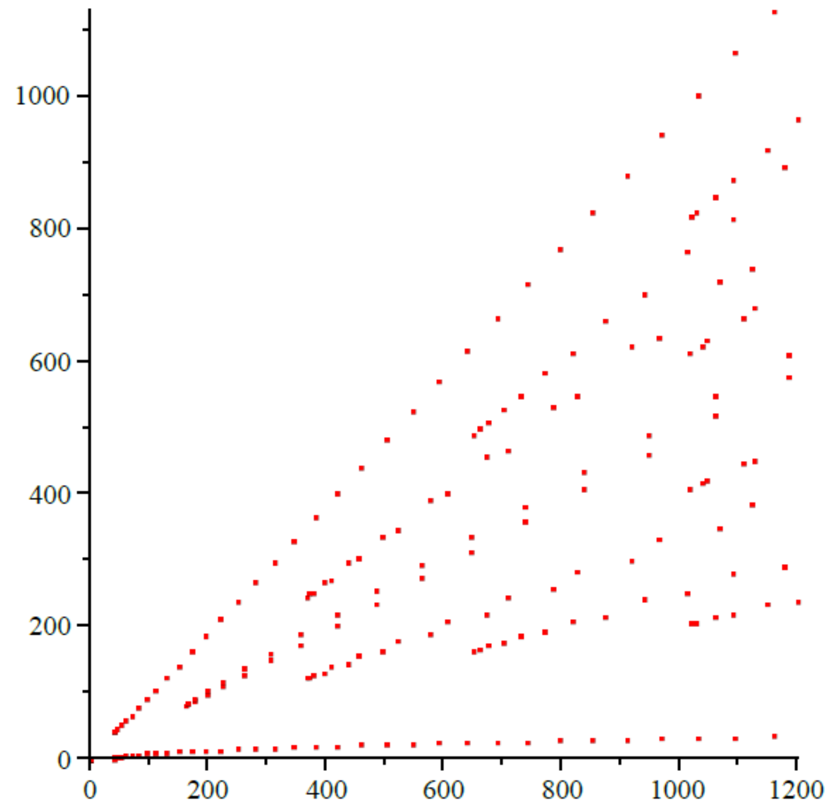
Graph of divisors
y^2 + y + 41 mod x ≡ 0



Note the exact curve fit of the parabolas to the divisibility points.

Graph with 10 parabolas

> $plot(x, y, style = point, symbol = point)$



Each of the 10 parabola on the previous slide can be matched with an expression on this page.

```
> h := n^2 + n + 41 :
> # Small equation coeffletents doublecheck
>
> y1d1 := factor(subs(n = z, h))
> y1d2 := factor(subs(n = z^2 + 40, h));
>
> y2d1 := factor(subs(n = 2 z^2 + z + 81, h));
>
> y3d1 := factor(subs(n = 3 z^2 + 2 z + 122, h));
> y3d2 := factor(subs(n = 6 z^2 + z + 244, h));
>
> y4d1 := factor(subs(n = 4 z^2 + 3 z + 163, h));
> y4d3 := factor(subs(n = 12 z^2 + 5 z + 489, h));
>
> y5d1 := factor(subs(n = 5 z^2 + 4 z + 204, h));
> y5d2 := factor(subs(n = 10 z^2 + z + 407, h));
> y5d3 := factor(subs(n = 15 z^2 + 4 z + 611, h));
> y5d4 := factor(subs(n = 20 z^2 + 11 z + 816, h));
```

$$y1d1 := z^2 + z + 41 \tag{1}$$

$$y1d2 := (z^2 + z + 41)(z^2 - z + 41) \tag{2}$$

$$y2d1 := (4z^2 + 163)(z^2 + z + 41) \tag{3}$$

$$y3d1 := (z^2 + z + 41)(9z^2 + 3z + 367) \tag{4}$$

$$y3d2 := (4z^2 + 163)(9z^2 + 3z + 367) \tag{5}$$

$$y4d1 := (16z^2 + 8z + 653)(z^2 + z + 41) \tag{6}$$

$$y4d3 := (16z^2 + 8z + 653)(9z^2 + 3z + 367) \tag{7}$$

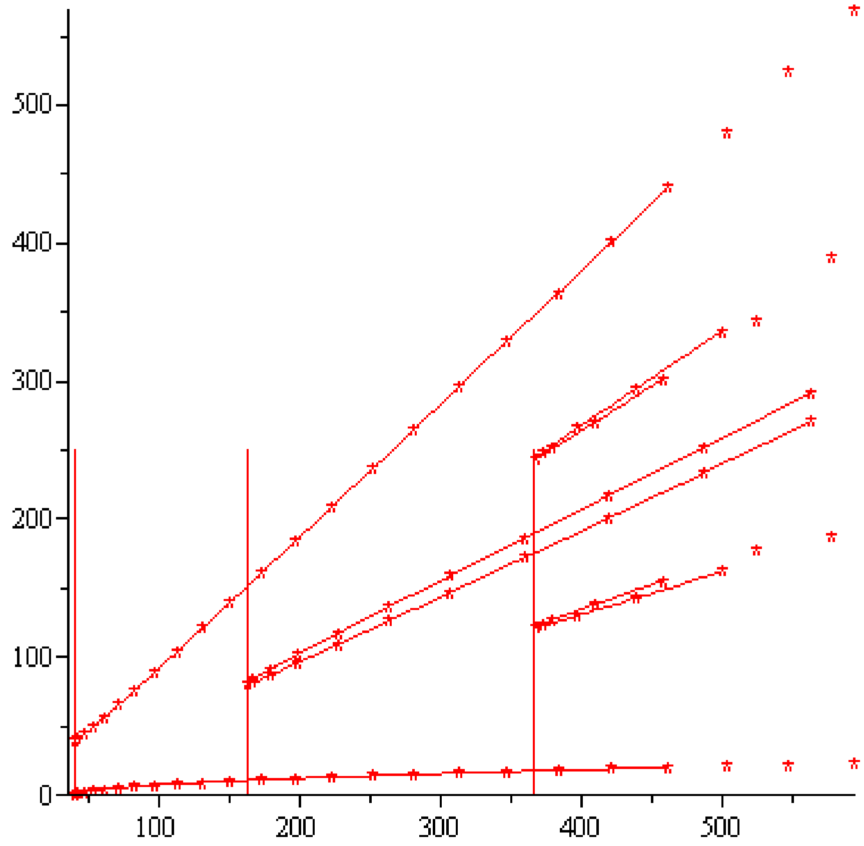
$$y5d1 := (z^2 + z + 41)(25z^2 + 15z + 1021) \tag{8}$$

$$y5d2 := (4z^2 + 163)(25z^2 + 5z + 1019) \tag{9}$$

$$y5d3 := (25z^2 + 5z + 1019)(9z^2 + 3z + 367) \tag{10}$$

Graph of divisibility

Vertical lines at 163*n^2/4



Notice the vertical lines are tangent to the parabolas.

A possible expression

Expression for the parabola at a given row and column

$p(r,c) = c^2x^2-2crxy+r^2y^2-(cr+1)x+r^2y+41r^2$.

Again $1<r$, $0<r<c$ and $GCD(r,c) = 1$.

Invitation to contribute

- If anyone is interested in working on this project with me, please let me know.
- Matt.c1.Anderson@gmail.com
- This project is similar to one of Landau's problems of 1912. Are there infinitely many primes of the form p = n^2 + 1? These problems are hard and unsolved.

Thank you

- Thanks to Colin Starr for allowing me to give this talk.
- Thanks to Peter Otto for useful suggestions on this project.
- Thanks to Willamette University for having an academic listener program to expose me to such a great topic.