

# A prime producing quadratic expression

By Matthew Anderson 2019

# An interesting quadratic expression

- $r(n) = n^2 + n + 41$  and assume  $n$  is an integer

Is prime for  $n = 0, 1, \dots, 39$

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.

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

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

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  $\pm 1$ .

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  $\pm 1$ .

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 on the next slide 😊)

**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  $\pm 1$ .

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.

This is a theorem and not a conjecture or an observation.

# First few values of $r(n)$

$n$	$r(n)$
0	41
1	43
2	47
...	
39	1601

By inspecting the table,

we can deduce that

$n^2+n+41$  is prime for

$0 \leq n \leq 40$

note that  $r(n) = n(n+1) + 41$ .

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





# Natural Numbers

- The natural numbers are 1, 2, 3, ...
- We will use only integers throughout this presentation.

# Divisibility by 2

- $r(n) = n^2 + n + 41$
- 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.
- $r(n)$  is always odd, no matter if  $x$  is even or odd.
- $r(n)$  is never divisible by 2.

# Divisibility by 3

Again  $r(n) = n^2 + n + 41$ .

There are 3 possible remainders mod 3.

0, 1, and 2

$$r(0) \bmod 3 = 2$$

$$r(1) \bmod 3 = 1$$

$$r(2) \bmod 3 = 2$$

Since  $r(n) \bmod 3$  is never 0,

$r(n)$  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  $r(n)$  is divisible by  $c$ , as long as  $n = r \bmod c$ .



# The “These Data Points Come in Pairs” Theorem about generalized $r(n)$

Let  $r(a) = a(a+1) + p$ .

Show that  $r(a) = r(-a - 1)$ .

Proof Because  $r(a) = a^*(a+1) + p$ .

Now  $r(-a - 1) = (-a - 1)(-a - 1 + 1) + p$ .

So  $r(-a - 1) = (-a - 1)(-a) + p$ .

And  $r(-a - 1) = (a + 1)a + p$ .

Thus  $r(-a - 1) = r(a)$ .

Which was what we wanted.

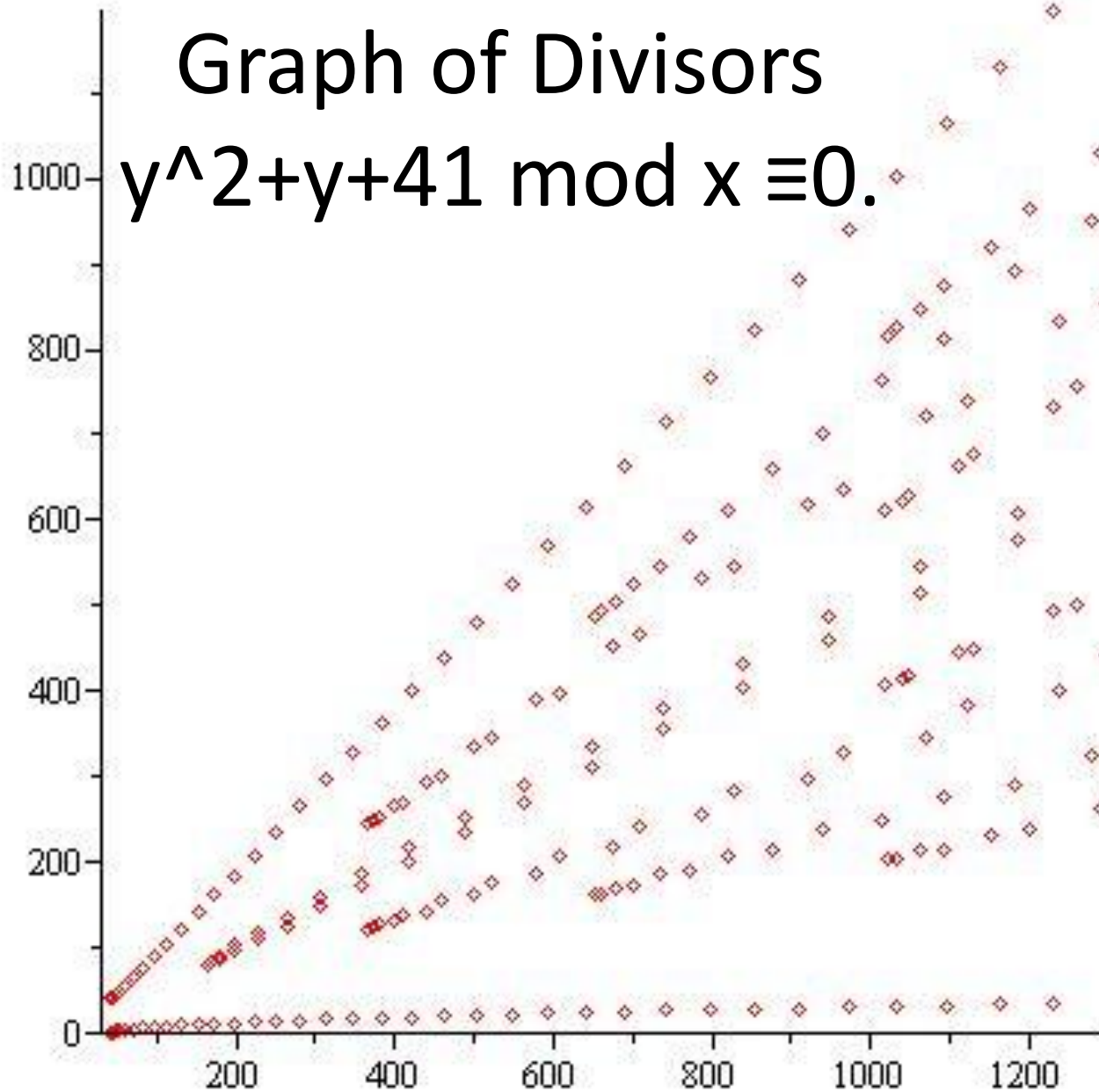
This means that, essentially, the data points come in pairs.

# From a lookup table to a graph

- The x axis is the divisors. 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  $r(y) \bmod x = 0$  then plot a point.
- Every time  $r(x)$  is composite, there is at least one corresponding point on the graph.

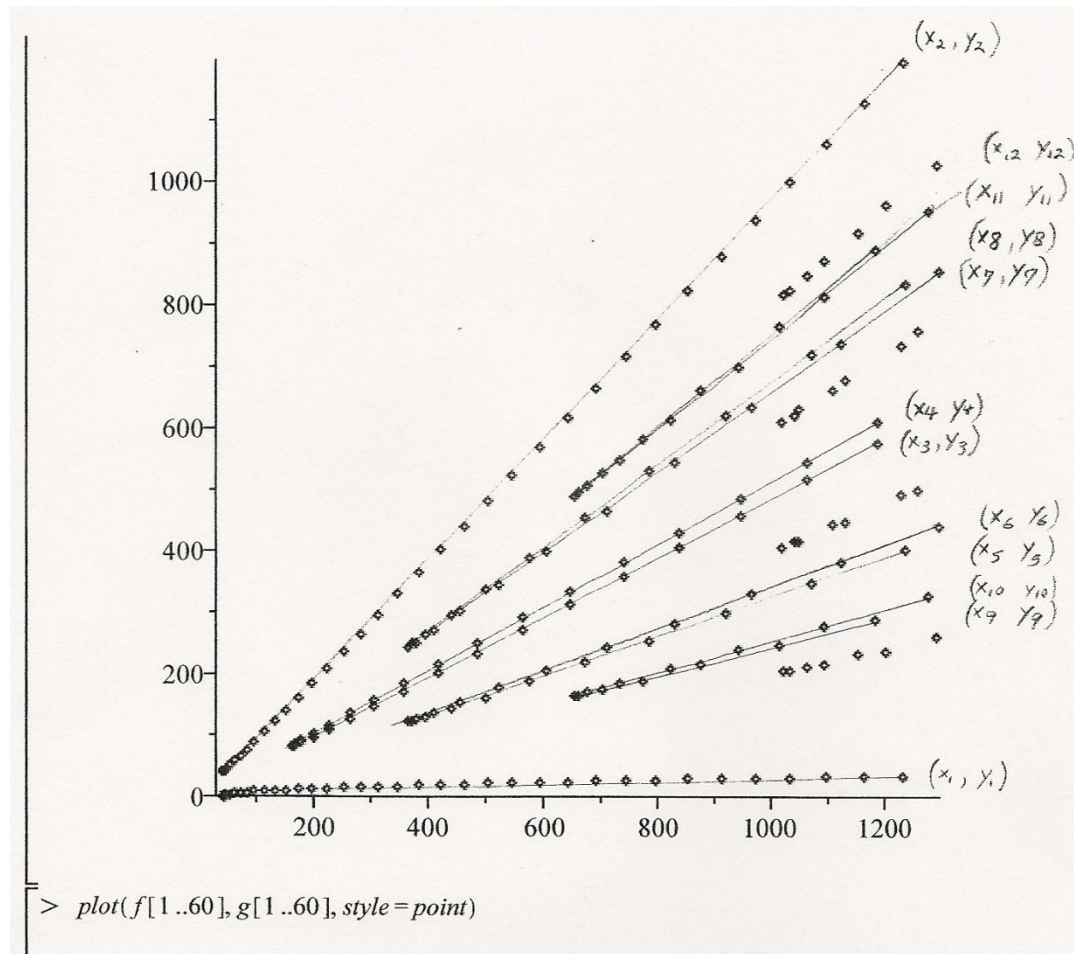
# Graph of Divisors

$$y^2 + y + 41 \pmod{x} \equiv 0.$$

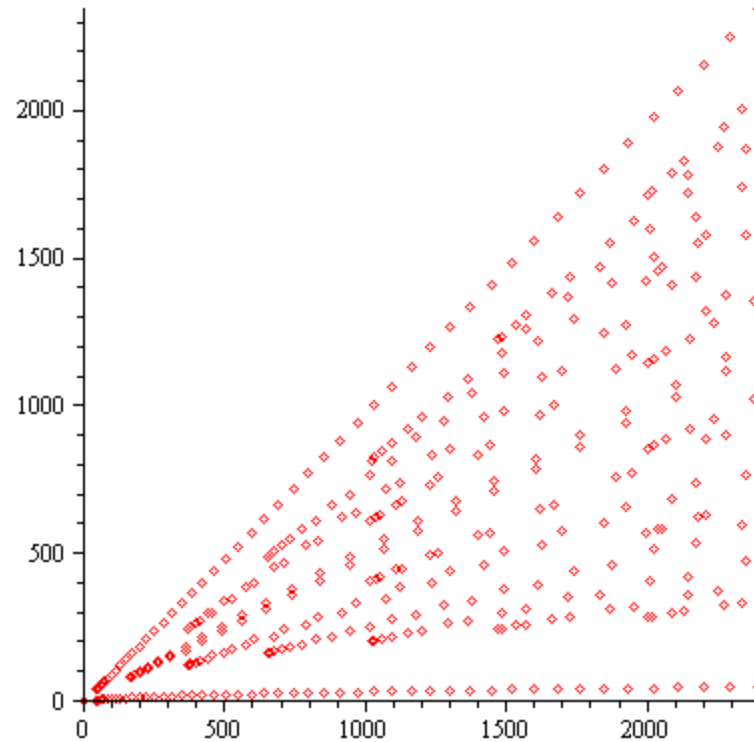




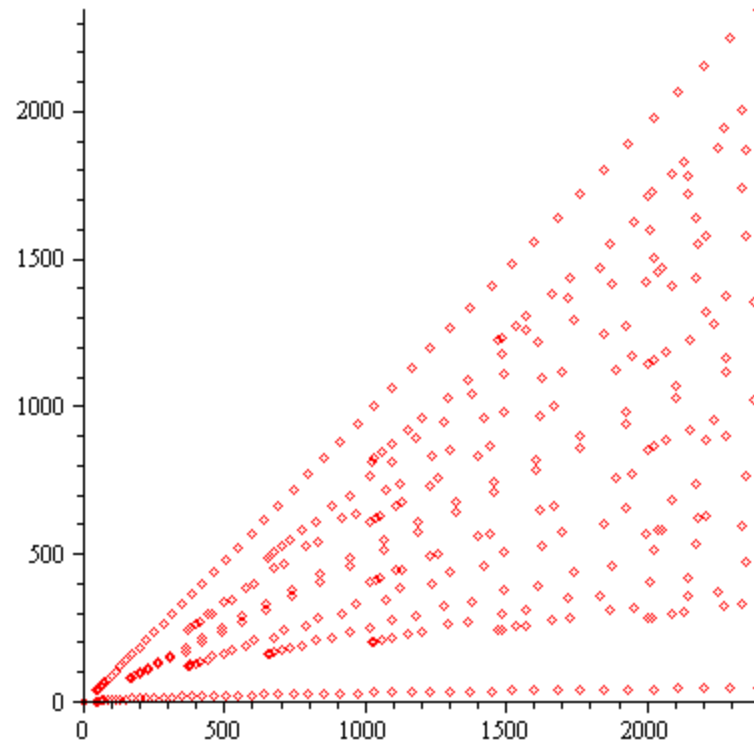
# Patterns in the graph of divisors



# Count the parabolas by columns

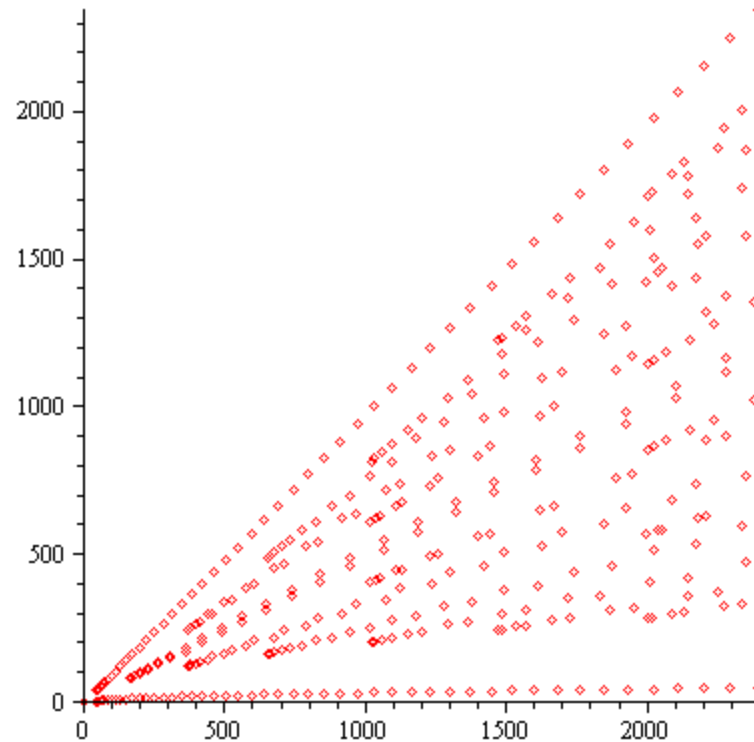


# Count the parabolas by columns



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](http://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

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

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.
- $r(x) = x^2 + x + 41$
- $r(y(x)) = (x^2+40)^2 + (x^2+40) + 41$
- $r \circ y(x) = (x^2+x+41)(x^2-x+41)$

This is a 4<sup>th</sup> order polynomial with algebraic factorization. It shows that under certain circumstances  $r$  is composite for all input  $x$ .

# Two more one parameter expressions

Use the technique of composition of functions

- $Y[3,1] = 2z^2 + z + 81$

$$x[3,1] = h(y[3,1](z))$$

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

$$Y[3,2] = 3z^2 + 2z + 122$$

$$x[3,2] = (9z^2 + 3z + 367)(z^2 + z + 41)$$

# Some Data from the graph

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

(41,0)

(41,40)

(43,1)

(43,41)

(47,2)

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

This would make  $r(x)$  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

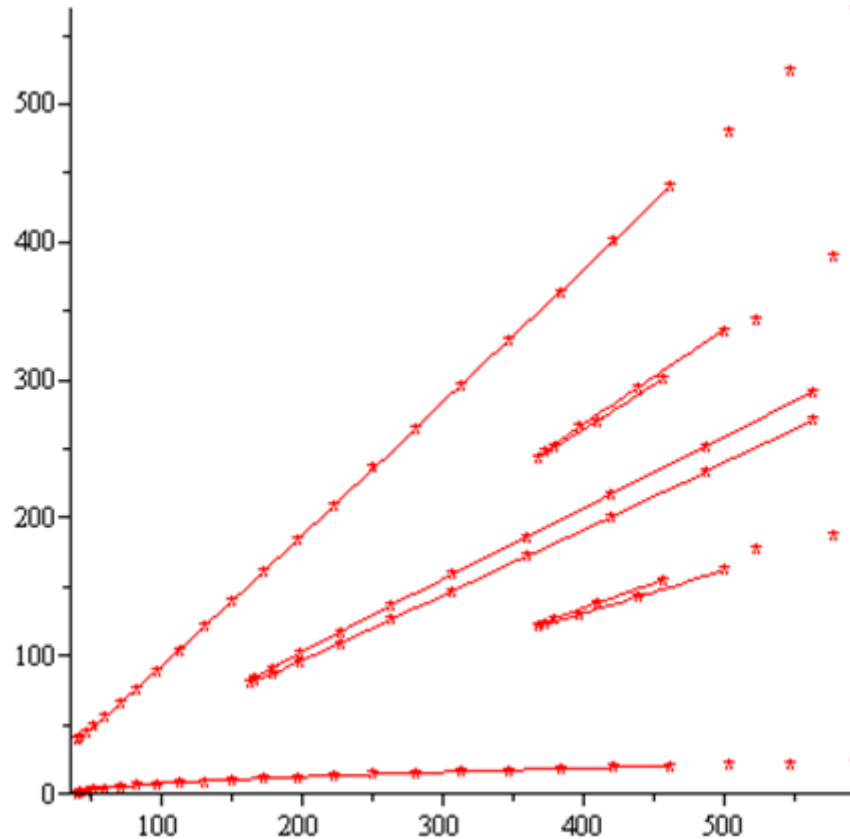
$h(n)$  is composite for all integers  $a$  and  $z$ .

see the [oeis.org/A201998/](http://oeis.org/A201998/)

# 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

$$y^2 + y + 41 \pmod{x} \equiv 0$$


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

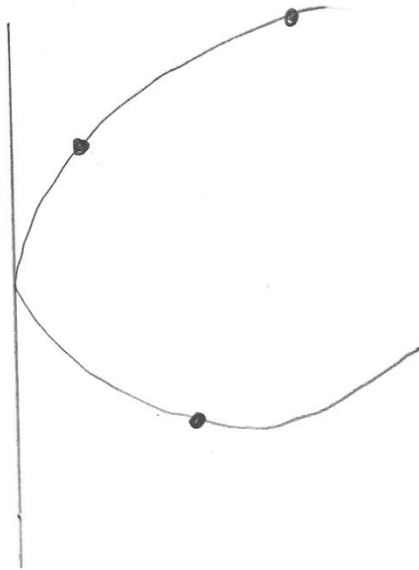
# Method of Quadratic Curve Fit

- Start with 3 data points.
- Solve a system of 3 equations and 3 unknowns.
- A generalized quadratic expression is

$$\text{Parabola} = A * x^2 + B * x + C.$$

# Method

Parabola and Minimum



Choose 3 data points.  
Introduce variable  $t$ .  
Use  $t = -1, 0$  and  $1$  and the  
Y part of the data point.  
Solve a system of 3 variables  
And 3 unknowns.  
Determine the expression for the  
Parabola.

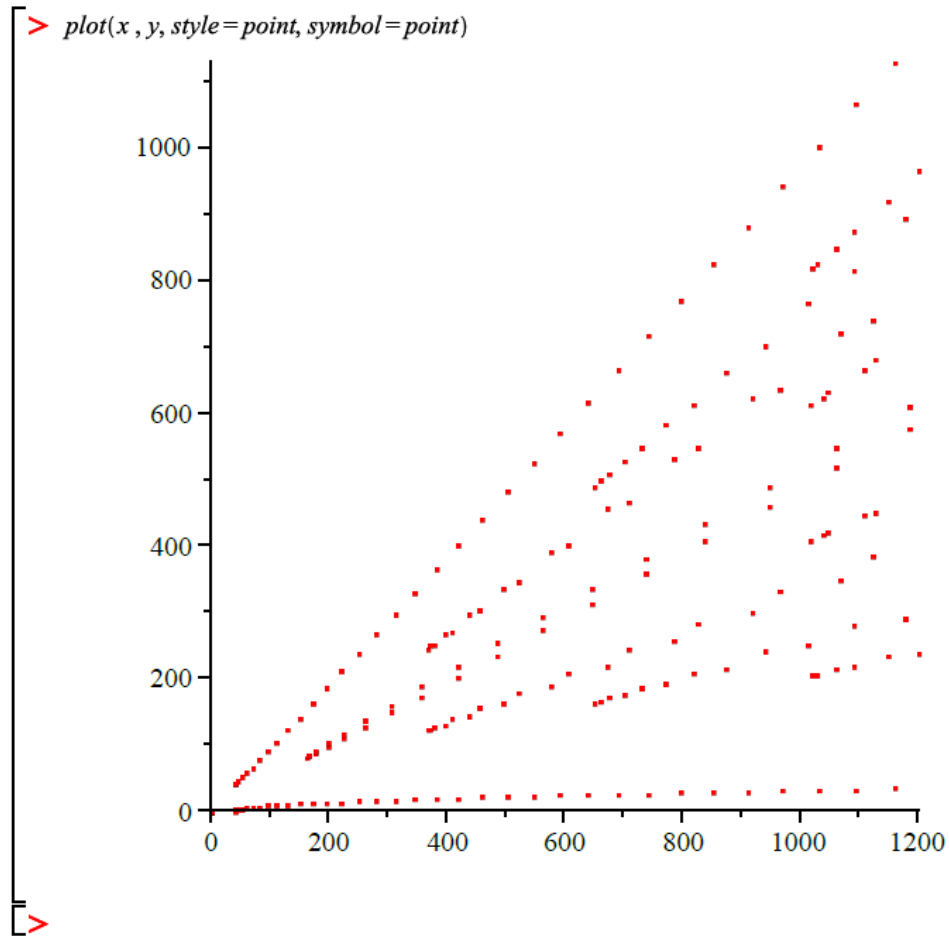
Repeat.

Horizontal minimum of parabolas is at  $163 \cdot x^2/4$ .

# Data points for $x^2 + x + 41 \pmod{y} \equiv 0$

	(x,y)
	0, 41
•	40, 41
•	1, 43
•	41, 43
•	2, 47
•	44, 47
•	3, 53
•	49, 53
•	4, 61
•	56, 61
•	5, 71
•	65, 71

# Graph with 10 parabolas



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

```

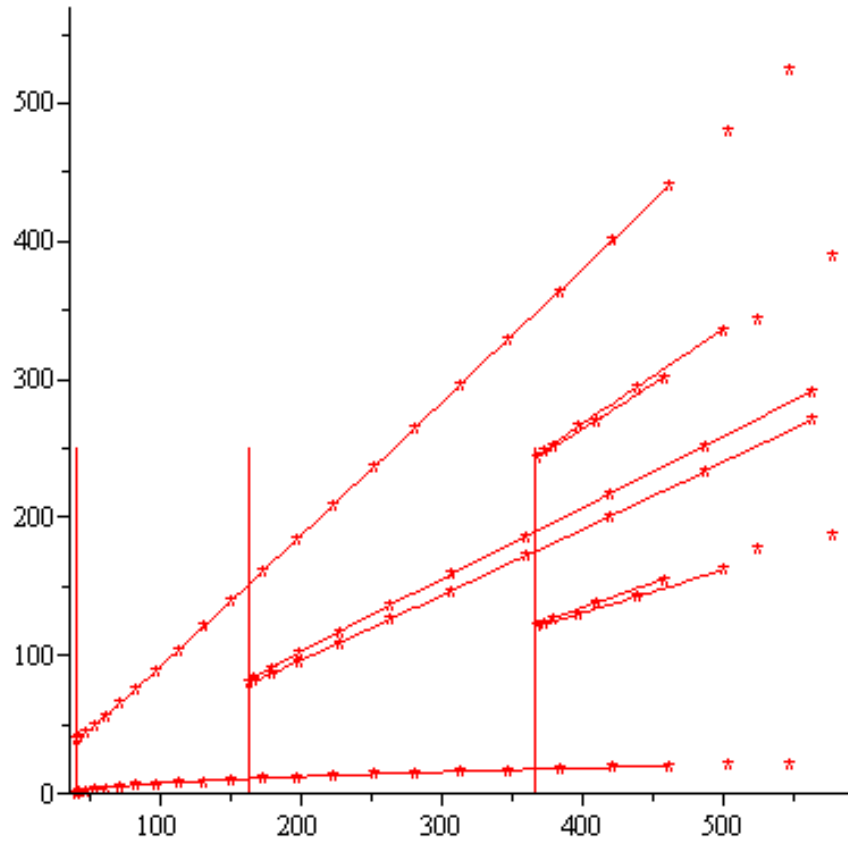
> h := n^2 + n + 41 :
> # Small equation coefficients doublecheck
>
> y1d1 := factor(subs(n = z, h))
                                     y1d1 := z^2 + z + 41
                                     (1)
> y1d2 := factor(subs(n = z^2 + 40, h));
                                     y1d2 := (z^2 + z + 41) (z^2 - z + 41)
                                     (2)
>
> y2d1 := factor(subs(n = 2z^2 + z + 81, h));
                                     y2d1 := (4z^2 + 163) (z^2 + z + 41)
                                     (3)
>
> y3d1 := factor(subs(n = 3z^2 + 2z + 122, h));
                                     y3d1 := (z^2 + z + 41) (9z^2 + 3z + 367)
                                     (4)
>
> y3d2 := factor(subs(n = 6z^2 + z + 244, h));
                                     y3d2 := (4z^2 + 163) (9z^2 + 3z + 367)
                                     (5)
>
> y4d1 := factor(subs(n = 4z^2 + 3z + 163, h));
                                     y4d1 := (16z^2 + 8z + 653) (z^2 + z + 41)
                                     (6)
>
> y4d3 := factor(subs(n = 12z^2 + 5z + 489, h));
                                     y4d3 := (16z^2 + 8z + 653) (9z^2 + 3z + 367)
                                     (7)
>
> y5d1 := factor(subs(n = 5z^2 + 4z + 204, h));
                                     y5d1 := (z^2 + z + 41) (25z^2 + 15z + 1021)
                                     (8)
>
> y5d2 := factor(subs(n = 10z^2 + z + 407, h));
                                     y5d2 := (4z^2 + 163) (25z^2 + 5z + 1019)
                                     (9)
>
> y5d3 := factor(subs(n = 15z^2 + 4z + 611, h));
                                     y5d3 := (25z^2 + 5z + 1019) (9z^2 + 3z + 367)
                                     (10)
>
> y5d4 := factor(subs(n = 20z^2 + 11z + 816, h));

```



# Graph of divisibility

Vertical lines at  
 $163 \cdot n^2/4$



Notice the vertical lines are tangent to the parabolas.

# Euler totient function

- Is the number of factors of a natural number.
- Is in encyclopedia [oeis.org/A000010](http://oeis.org/A000010).
- Sequence starts 1,1,2,2,4,2 and so on.
- Is the count of the number of parabolas in a column.

# Invitation to contribute

- If anyone is interested in working on this project with me, please let me know.
- [Matt.c1.Anderson@gmail.com](mailto: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 at Willamette University.
- Thanks to Peter Otto at Willamette U. for useful suggestions on this project.
- Thanks to Chris Sinclair at the University of Oregon for assistance.