THREAD:
DOES ANYONE KNOW ANY MODULUS ATTACKS IN RSA?

02-28-2012, 09:02 PM #11

trurl_
Registered User

Join Date: Dec 2004
Posts: 133

KNOWING HOW TO FIND 6TH ORDER POLYNOMIAL WILL MAKE RSA 2 WAY FUNCTION

I think this may be something. I only tested one value, but it applies to all factors. Did anyone see this from what I posted last time?

http://www.constructorscorner.net/id.../RSA2Lane.html

Could be nothing. Will only take a minute to determine if it is something.

It's all about ideas.

constructorscorner.com

Blog this Post | Edit Post | Reply | Reply With Quote

04-21-2012, 01:36 AM #12

trurl_
Registered User

Join Date: Dec 2004
Posts: 133

HOW DO I PROGRAM AN ANSWER IN MATHEMATICA AS A VARIABLE WHEN IT HAS MULTIPLE ANSWERS?

Code:

```
p = 85^4/((85^4/x)+ 2*85^2*x^2 +x^5) - 5

sol = NSolve[p   0]

-5+52200625/(52200625/x+14450 x2+x5)

{{x  10.7235 +26.6243  },{x  10.7235 -26.6243  },{x  -22.8216+10.9987  },{x  -22.8216-10.9987  },{x  19.0002},{x  5.19606}}
```

Does anyone see a pattern now?

My question is how to analyze the data by programming. NSolve gave decimal numbers but only 2 are true. Really only 5 is true. I think 19 is close enough to 17 that 85/19 = 4.7 .

If you think about it something that doesn't have a pattern with symmetry and proportions as a shape like a parabola has, can only be described by higher order polynomial equation, because it allows for variation. The trouble is solving those polynomials.

I want more analysis. I need the answer for NSolve in a variable so I can do calculations with this. I can do calculations in Mathematica I just can't program. Is there any way to program such intangible data? Help would be much appreciated.

It's all about ideas.

constructorscorner.com

Blog this Post | Edit Post | Reply | Reply With Quote

04-21-2012, 05:52 PM #13

trurl_
Registered User
Join Date: Dec 2004
Posts: 133

WOLFRAM ALPHA

I don't know how to seperate the variable in Mathematica when there are several answers. Is it like an array?

Did anyone ever try Wolfram Alpha?

http://www.wolframalpha.com/input/?i...Bx%5E5%29+-+5+

It's all about ideas.

constructorscorner.com

Blog this Post | Edit Post | Reply | Reply With Quote

trurl_
Registered User
Join Date: Dec 2004
Posts: 133

UPDATE 7-3-12

I recently submitted my logarithmic spiral and Prime number pattern to 2600 magazine. Obviously unproven math theories are not as interesting to put in the magazine when compared to the philosophy of pirating movies and software. I may have chosen the wrong audience, but the magazine is more politics and less technical. Most outlets, 3DBuzz excluded, advertise tech and design then waste the reader's time with arguments on politics and religion. I know what I believe, but I don't know the latest programming techniques. I want to see something designed and not argue what it means to be a hacker. 2600 magazine has its strong points, but the point is lost when the content is not about actual projects. I see the same articles. Reading a 3 page article on what it means to be a hacker which was rehashed from last quarter is not sharing any relevant information. My math is imperfect, but to me it was always about the concept. I would rather work at a math project that didn't work than to try to justify why it is important to pirate intellectual content, like is done every issue of 2600.

If my math problem did work, Prime numbers could no longer be used in public key cryptography. Theoretically, any series a numbers in a pattern could be solved. This would not destroy encryption though. The trick would be to have a polynomial that could not be solved. I don't know off hand how we would find such polynomials. But we need to find better ways to solve polynomials. It is this roadblock that we find useless equations that result in not being able to substitute and solve equations.

The reason I used substitution in finding the 2 Prime products was to solve them only using algebra. However, it is impossible not to be faced with the fact that without 2 distinct equations, an always true equation results. To fix this I relied on similar triangles. Where do the similar triangles come from? You guessed it: the logarithmic spiral. We can use similar triangles without knowing where or what kind of logarithmic spiral we have.

But there is more. Just going by intuition I believe this logarithmic spiral can be used to solve for polynomials. The polynomial equation is directly related to the spiral. For example, if we have a logarithmic spiral where all Prime numbers occur at an unknown distance along the spiral but at the same proportionate angle along all Prime numbers, the logarithmic spiral could be solved for. But more importantly we have a geometric visual representation of a polynomial. This visualization is much better than the chaotic graph we have with irrationals and imaginary numbers.

Again, all of this is unproven. Which is why 2600 didn't see any potential in my article. So if you have read my theory which is just simple algebra and you see something or not let me know. I have not posted much

new content to my website lately, but this idea is here before I post anything to support it.

I strongly believe that finding polynomials is the key to finding Prime numbers. And if someone ever finds a way to reverse the one way function of Prime multiplies, polynomials which can't be simplified will be the next one way functions that public key relies on. Of course I could be full of it. But you must admit this is one powerful concept.

It's all about ideas.

constructorscorner.com

Blog this Post | Edit Post | Reply | Reply With Quote

07-03-2012, 08:38 AM #15

ZanQuance
ScumSoftware

Join Date: Sep 2006
Location: Polysorbate 60
Posts: 926

Please stop all that shouting, it's making people nervous...

42

Blog this Post | Reply | Reply With Quote

07-04-2012, 07:52 PM #16

trurl_
Registered User

Join Date: Dec 2004
Posts: 133

Sorry. I was having trouble getting the format to paste.

It's all about ideas.

constructorscorner.com

Blog this Post | Edit Post | Reply | Reply With Quote

07-21-2012, 07:52 PM #17

trurl_
Registered User

Join Date: Dec 2004
Posts: 133

On Wolfram.com website there is a free plug-in to play CDF interactive documents.

The particular one I looked at recently in trying to find examples of logarithmic spirals and how we can find an equation of a spiral is:

http://demonstrations.wolfram.com/Sp...xponentiation/

The purpose of this Mathematica demonstration was to show iterating exponents. But I saw something more important: The spiral that is created is easily seen to be made of equilateral triangles. This is so apparent in this example that I don't know why it wasn't commented on.

To me when I think spiral, I see this even before I looked at the different drawings. So a line would connect the Prime numbers of a logarithmic spiral. That is if the spacing of the Prime numbers on the spiral fell at the same angle of all the other Prime numbers and was contained on the logarithmic spiral itself.

The next step is to solve the geometry of the logarithmic spiral. Why? Because we do not have a starting point to solve polynomials in an easy way, so we look to the geometry. When you look at encryption you see that all the one way functions are protected by polynomials. The one way function would be easy if you did not get impossible equations when trying to use algebra and substitution. In fact from what little I know of elliptical cryptography, it is based on irreducible, factorable polynomials.

My advice for impossible problems such as Prime number pattern or Prime number multiples is to start with the geometry. Similar triangles forming a spiral is the place to start when all existing equations lead nowhere.

I am looking at others work on Wolfram.com and exploring the examples because they are so visible. But when I see something like in the link I posted, I hope there is something true about my own work. I can only look at my Prime number work for so long. Even if you are not interested in my problem, I recommend Wolfram and Wolfram Alpha if you are interested in math because of the interesting shapes and problems presented there.

It's all about ideas.

constructorscorner.com

Blog this Post | Edit Post | Reply | Reply With Quote

07-29-2012, 04:56 AM #18

trurl_
Registered User

Join Date: Dec 2004
Posts: 133

Ok, my next step is to geometrically describe the logarithmic spiral. It is important to remember this is just a concept. If you put too much effort into an impossible question you will surely be disappointed if you do not find instant solutions.

This problem I have been recording here at 3DBuzz leads to more and more impossible solutions. I think there is more to learn by trying the impossible than to use conventional methods. Don't get me wrong mathematical fundamentals have the place especially when you are taking a math course, but a math experiment is much more fun.

As you see from the Mathematica Demonstration on the Wolfram site there is a bunch of equilateral triangles revolving or orbiting around the origin or center. I think there is order here. This order can be used to solve the equation of the logarithmic spiral.

Of course, we must test it. I like this problem because it seems impossible. It is only impossible because we do not understand it. Obviously we must look at the problem in simple steps to understand what is going on.

It is late as I write this so my description will be brief and to the point.

I think we can solve these rotated similar triangles. I am just stating a theory. If the radius of the spiral changes as it rotates we should be able to find this rate of change. This is much easier seen geometrically than by equations. If we set the changing radius to points where the radius equals a Prime number (in order) and we use the fact that we can determine some sides of the triangles that rotate, we may have a simple way to explain the overall points we need.

I know this post is jumbled. I am tired and just want to record this idea. I am going to introduce a problem that may discredit my work. In fact it created a lot of criticism when I posted it to a science forum a few years ago.

Side Angle Side

Side Side Side

Angle Angle Side

http://www.scienceforums.net/topic/4..._1#entry503263

I haven't looked at this in a few years so I will have to review it. But it is interesting to read, even if you want to see them bash my post. BTW it is www.constructorscorner.net now and not .com

Now this is a math problem. You might even start to think it works. The claim is bold, but the technique is more practical once you read it. I am not claiming it works. I am just using it as a tool to think of how we can draw this logarithmic spiral.

I will update this post with more info in the next few days.

Remember don't be discouraged by the claim of knowing only 2 sides. The write up is more practical.
See the "Trig Parabola" post at

http://www.constructorscorner.net/id.../math_home.htm

It's all about ideas.

constructorscorner.com

Blog this Post | Edit Post | Reply | Reply With Quote

07-31-2012, 06:23 PM #19

trurl_

Join Date: Dec 2004
Posts: 133

Registered User

I am not claiming the 2 sided triangle works. Yes, I know that 2 side of different lengths equal infinitely many triangles. That was never what I was saying.

I was saying that 2 know lengths and a known angle opposite those lengths can be solved. I suggested finding the right triangle that the 2 lengths would fit.

So with this solved triangle there still be an unknown triangle but you would know the reference triangle which shares the sides of the unknown 2 sided triangle. So with some more values of the unknown triangle (such as similar triangles or another angle being known) it may help solve a triangle that would otherwise have too little information. Thus that name of the thread was “Two Sided Triangle”.

I never intended to say 2 sides could determine a unique triangle by themselves. That doesn’t even make sense. I wanted the scientists of SFN to look at my concept because they are more mathematically knowledgeable. I thought a scientist would be more objectionable, but they never got past the name of my post.

I am not saying it works. I am saying if it was possible it would be useful and just consider the concept. I know 2 sides don’t determine a triangle. I know that it isn’t clear why we need such a solution, but I will try to describe more in a future post.

It's all about ideas.

constructorscorner.com

Blog this Post | Edit Post | Reply | Reply With Quote

08-12-2012, 04:23 AM #20

trurl_
Registered User

Join Date: Dec 2004
Posts: 133

CAN ANYONE FIND MULTIPLE VALUES OF THE LENGTH OF THE 2 SIDES OF A TRIANGLE THAT HAS A

Can anyone find multiple values of the length of the 2 sidesof a triangle that has a hypotenuse of 3?

Click Here!

If my trig parabola was correct you shouldn’t be able to. It would also mean that Prime numbers when the length of the hypotenuse only have 1 set of adjacent sides that are possible to complete a right triangle.

Of course this is just a concept; I have not done the math yet. But you could prove me wrong by finding the possible sides of a hypotenuseof 3.

It wouldn’t matter if it is proven wrong. It would just mean my effort didn’t produce accurate results. But as long as there was a triangular reference for the Prime number radius of a logarithmic spiral, the logarithmic spiral equation could be set equal to itself as a proportion. Again I haven’t done the math. I just want interest in the problem.

Look at the trig parabola simplified PDF and judge for yourself. I know the equation is cubic. However, treating it as quadratic worked. I verified the solution on Wolfram Alpha. I believe if a large even number was plugged into the trig parabola equation more real results would be found. This would mean the number isn’t Prime (it is even) and this is one very confusing way to look at a triangle. It seems like it should not be possible.

But even if it doesn’t work the method of the trig parabolawould still be a great way to organize Prime numbers along a logarithmic spiral.

If you have been following along with my post, please let meknow if you saw any potential in my posts. If you read the last post you saw that my ideas were not accepted. But keep in mind that this is a concept. It is virtually impossible to find a pattern to Prime numbers. I am just showing a way to think of this possible pattern. All it is basic geometry. It might be true that I put a lot of effort into it. But I am learning as I go and reviewing math concepts at the same time. I know you should have some heavy math under your belt before research. Don’t laugh  I know if this were a degree I would have much difficulty defending my work. That is why it is a concept; an approach to a problem. I want to approach a meaningful problem and have there be thinking. I don’t want to only go by the textbook.

It's all about ideas.

constructorscorner.com

Blog this Post | Edit Post | Reply | Reply With Quote

+ Reply to Thread

QUICK REPLY

Font Size

Show your signature

Post Quick Reply Go Advanced Cancel

« Previous Thread | Next Thread »

TAGS FOR THIS THREAD

None
View Tag Cloud

Add / Edit Tags

POSTING PERMISSIONS

You may post new threads
You may post replies
You may post attachments
You may edit your posts

BB code is On
Smilies are On
[IMG] code is On
[VIDEO] code is On
HTML code is Off

Forum Rules