

Forum Programming C and C++ New One Way Function

+ Reply to Thread

Page 2 of 2 First 1 2

Results 11 to 20 of 20

THREAD:
NEW ONE WAY FUNCTION

10-06-2013, 12:59 AM

#11

 trurl_ 
 Registered User

 Join Date: Dec 2004
 Posts: 137

CORRECTED AND EASY TO SEE

Code:

```

y = sqrt[(((85/x) * 85 - x^2)/ x) ] = ((85^2/x) + x^2)/ 85
In[27]:=
p = (((85/x) * 85 - x^2)/ x - (( 85^2/((85^2/x) + x^2) ) ^2));
sol = NSolve[p == 0, x]
Out[28]= {{x -> -36.2894}, {x -> 27.7376 + 21.7226 I}, {x ->
27.7376 - 21.7226 I}, {x -> -10.093 + 32.5167 I}, {x -> -10.093 -
32.5167 I}, {x -> 9.44493}, {x -> 0.257048 + 9.23565 I}, {x ->
0.257048 - 9.23565 I}, {x -> -8.95875}}

```

This is still an approximation. In the above example 9 solves the equation better than 5. That is where 5 should be the desired answer. $N = 85$; $x = 5$; and $y = 17$. So there still isn't a perfect solution just estimated. But take:

```

In[31]:= y = sqrt[(N * y - x^2) / x]
y = sqrt[(7872197 * 3191 - 2467^2) / 2467]
Out[31]= sqrt[(-x^2 + N sqrt[(-x^2 + N sqrt[(-x^2 + 1/85 N (7225/x + x^2))/x])/x])/x]
Out[32]= sqrt[10180014]
So sqrt of 10180014 = 3190.613421 which is approx y or 3191.

```

It's all about ideas.

constructorscorner.com
 Blog this Post

 Edit Post
  Reply
  Reply With Quote

10-18-2013, 09:22 AM

#12

 KareemSharrock 
 Registered User

 Join Date: Oct 2013
 Location: Chicago
 Posts: 5

thats a nice way to denote the query here, i just love it a lot the way you have represented to us this thing...

 Blog this Post

 Reply
  Reply With Quote

10-20-2013, 01:00 AM

#13

 trurl_ 
 Registered User

 Join Date: Dec 2004
 Posts: 137

HELP ME PROGRAM THIS DARN PROGRAM!!!

I know no one believes in my simple product of 2 numbers. The equations are approximations. There is a numerical margin of error in the answer.

I have been plugging in values into Wolfram Alpha ; just plugging and chugging. But do not doubt that my original equations, though only using simple algebra were not thought out.

Mathematica solves for the complete equation when I want to know x. That is why I isolated x.

But if you do not believe me look at this link to Wolfram Alpha. The Key or N is 7 digits and when you place the values into the equation it approximately equals zero or 0.996689381502487424655039628983612683803467839089 3290

The problem is I need a computer algorithm or a way to program Mathematica to find what I want.

I am not a good programmer. So I am requesting the help of anyone who reads this thread.

Is there any value to have an approximation of values that are candidates to being the Prime products?

Even if it had a margin of error an approximation would greatly reduce the factoring. That is you would only have to test odd numbers and could eliminate non-Prime numbers by other means.

So I request some guidance here. Does anyone see value? I have been told I am bashing my head against the wall with impossible problems. But I do not choose a problem because it is impossible, I choose a problem based if I feel I have a unique approach.

But actually solving the polynomial is where the problem occurs.

$$\left(\frac{((7940729^2)/2297)+2297^2}{7940729} - \left(\sqrt{\frac{((7940729/2297)*7940729-2297^2)}{2297}}\right)\right) = 0.996689381502487424655039628983612683803467839089 3290$$

Where N = 7940729

p = 2297

e = 3457

$$\left(\frac{((7940729^2)/2297)+2297^2}{7940729} = 3457.6644$$

$$\left(\sqrt{\frac{((7940729/2297)*7940729-2297^2)}{2297}}\right) = 3456.6677$$

There are many possible differences in the derived equations, but basically we are searching for the easiest to solve and most accurate.

I believe we need to find the margin of error for the sqrt approximation. It may be the same for all values.

But again I ask if you have any interest in this problem help me program a solution.

<http://www.wolframalpha.com/input/?i...F2297%29%29%29>

<http://www.wolframalpha.com/input/?i...F2297%29%29%29>

It's all about ideas.

constructorscorner.com

 Blog this Post

 Edit Post |  Reply |  Reply With Quote

10-24-2013, 02:40 AM

#14

 **trurl_**
Registered User

Join Date: Dec 2004
Posts: 137

Does anyone see anything? So if you are searching for 3457, you could round the numbers before subtracting. But I recommend finding the "error" of the approximation of the 2 equations that are subtracted.

So when you subtract the equations you are looking for a value > 0 and < 2

I am also looking for a reputable RSA encryption program. Any recommendations?

It's all about ideas.

constructorscorner.com

Blog this Post

Edit Post

Reply

Reply With Quote

10-25-2013, 12:34 AM

#15

BillSimpson 
Registered User

Join Date: Oct 2013
Posts: 1

Going back to your first post in this conversation, if two clocks are running at different speeds then they must show the same time at some point and must do this again and again. If one is gaining on the other then it must catch up and pass and then catch up and pass again and again. Mathematica or WolframAlpha can show your two clocks crossing about four times a week, paste this to see it. That uses Mod to make each clock "wrap around" at midnight.

```
Plot[{Mod[2 + 15/60 + 50/60 x, 12], Mod[7 + 21/60 + 67/60 x, 12]}, {x, 0, 168}]
```

Going back to your posts about multiples of decimal numbers being integers, if there is one digit after the decimal place then integer multiples of that will be an integer at least one out of every ten times, two digits after will be an integer at least one time out of every hundred times, etc.

For a "reputable RSA encryption program" you have to decide who you want to trust. Since it is only a few lines of code to do this yourself if you have a tool that can handle very large integers and provide a power mod operation, you might consider writing that yourself, testing it repeatedly and then hoping the result is safe and correct. You can Google for rsa decoder and find lots of web pages that will do this for you, but can you trust them or not?

And now to the big point. If you would like to take a little time to think about it and then sum up in a really really clear sentence or two what the goal is that might help me understand. Imagine you only have a moment of someone's time and attention and you need to explain the whole idea in a sentence so that they will understand exactly what you are planning. Assume the person who is hearing this understands math and math programming, but has no idea of any of the ideas in your head or all the things you have tried. Work on that sentence until you really think it explains the goal.

After you have that written and revised and improved and simplified and clarified then you might think about maybe two more sentences that ask to be given something clear and specific. Try to figure out a way that the person reading this will know exactly what it is that they are supposed to do and how they will know when they have it.

I understand you are still hunting for the answer and don't know what it will be yet. That is fine. If you can explain clearly what the goal is and how someone could know what direction to go looking and how they would tell if they found it, or something closer to it, then that would probably help a lot.

Thanks

Blog this Post

Reply

Reply With Quote

10-26-2013, 07:04 AM

#16

KareemSharrock 
Registered User

Join Date: Oct 2013
Location: Chicago
Posts: 5

could anyone explain about it clearly to me, i loved it a lot it would be helpful one for us to see.

Blog this Post

Reply

Reply With Quote

11-21-2013, 02:23 AM

#17

trurl_ 
Registered User

Join Date: Dec 2004
Posts: 137

Ok here is how this works. I am using plain substitution to find the 2 products that make up N.

So I formed many simple equations to explain x (the smaller of the 2 products) as according to y.

x and y can be found by finding when one is known. This proves the equation is true but isn't very useful because if I knew either x or y there wouldn't be any difficulty in the one way function.

But for this equation:

$$\text{Sqrt}[\frac{85*(85/x) - x^2}{x}] - ((85^2/((85^2/x) + x^2)) ^2) = 0$$

Solve for x

<http://www.wolframalpha.com/input/?i...+%5E2%29+%3D+0>

I am getting 4.5 which is in the range of error. I would have to test more and larger products, but I just know to be useful I have to solve a polynomial equation. The equation above is the simplest so far. I am not plugging and chugging. Ok maybe a little, but my equations are based on substitution. It is easy to make equations, the difficulty is solving the polynomial. I have many attempts and approaches but I want to keep it as simple as possible.

To help me program in Mathematica I requested help on a message board, but this is currently as close I came to something useful.

http://community.wolfram.com/groups/..._auth=Ga7Am322

It's all about ideas.

constructorscorner.com

Blog this Post

Edit Post | Reply | Reply With Quote

12-01-2013, 03:06 AM

#18

trurl_
Registered User

Join Date: Dec 2004
Posts: 137

ANOTHER RELATIONSHIP BETWEEN X AND Y

Using vector addition I have another equation. I can keep making these and maybe I will find a helpful relationship. But it does no good to find an equation in polynomial form if I cannot solve for x in the polynomial.

This time I keep it simple. My question is does this accomplish anything?

$$\text{Abs}[\tan(y / (2*\text{Pi}))]*x+x=(y ? ((2*\text{Pi})))$$

in radians of course

It's all about ideas.

constructorscorner.com

Blog this Post

Edit Post | Reply | Reply With Quote

12-01-2013, 04:36 AM

#19

trurl_
Registered User

Join Date: Dec 2004
Posts: 137

$$\text{ABS}(\text{TAN}(85 / (2*\text{PI}))) * X + X = 85/(2*\text{PI})$$

$$\text{Abs}(\tan(85 / (2*\text{Pi})) * x + x = 85/(2*\text{Pi})$$

Don't believe me look here:

http://www.wolframalpha.com/input/?i...%5F%282*Pi%29

It's all about ideas.

constructorscorner.com

Blog this Post

Edit Post | Reply | Reply With Quote

12-03-2013, 03:23 AM

#20

trurl_

Join Date: Dec 2004

IN RADIANS A VECTOR

Abs [tan (85/ (2* Pi))] * x + x^2 = (85/(2*Pi)) in radians

Here is the corrected equation. I think it gives an estimation of where the products occur.

Abs [tan (85/ (2* Pi))] * x + x^2 = (85/(2*Pi))

This is how I did the vector addition:

We know we have 2 vector sides x and y. But a triangle with those sides will not be large enough in most cases to have a resultant of 85.

So we start at a vector with length x starting at the origin and having a cosine of 1. Or just length x.

And to it another vector of length x at an angle in radians that starts at the origin and unravels to a length of y. so it is an angle that in some cases is greater than 360 or 720 or even revolving around the origin many times.

But the important thing to remember is that this angle is N/x also known as y.

The only reason 2 Pi is used is so we can find a similar triangle and the length of both sides of the triangle we are using to compute, stays of length x.

So we have a vector with 2 sides that equal x and the angle between the y/2*Pi.

And I must say that if we used other lengths larger than x it would need to be a triangle similar to this one we computed. You might even be able to picture a logarithmic spiral.

There are many equations we can make knowing the sides and angles. The only problem is can we solve the resulting equation?

This is just a brief description. I am working on a write-up. But I need to be sure this works or is even useful.

It's all about ideas.

constructorscorner.com

Blog this Post

Edit Post | Reply | Reply With Quote

+ Reply to Thread

Page 2 of 2 | First | 1 | 2

QUICK REPLY

Show your signature

Three empty input fields for user information.

« 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](#)

Powered by vBulletin®
Copyright ©2000 - 2013, Jelsoft Enterprises Ltd.

Services

[Live Classes](#)
[Workshops](#)
[Subscriptions](#)
[Support](#)
[Contact Us](#)
[About 3D Buzz](#)

News

[Company Blog](#)
[Newsletter](#)

Community

[All Forums](#)
[General Discussion](#)

Connect

[Become a fan](#)
[Follow Us](#)