THREAD:
DOES ANYONE KNOW ANY MODULUS ATTACKS IN RSA?

10-02-2012, 01:35 AM #21

trurl_
Registered User

Join Date: Dec 2004
Posts: 133

Hello again.

I would like to shout out of thanks to Stealth Coder. He told me I must have mathematical evidence. I hope I can convince him that there was not a waste to my math research project. Sometimes you find nothing and other times there is a little thing that made your effort worthwhile. I hope to convince someone to write a program for this.

On a logarithmic spiral exist Prime numbers. If the spacing is one revolution or 2Pi then we can easily find a pattern to primes. The revolution of the Primes does not matter as long as they are in the same angle (which is similar triangles.)
The pattern where x is the start Prime number and y is the next Prime number in the series.

(X^2*y^4 + x^3*y^2 + x^2*y^2 + x^3 – x^3*y^3) divided by (x^2*y^3 + x^3*y)

For x = 5 and x = 7 this equals 2.60

Where 7 – 5 = 2

The difference is due to the angle between 5 and 7

The pattern is always there. Why just didn’t have a mathematical way to describe it before.

I will follow up on this. I have to test and write up to my site.

Thanks for looking,
Trurl

It's all about ideas.

constructorscorner.com

Blog this Post Edit Post Reply Reply With Quote

10-02-2012, 02:08 PM #22

stealthcoder
Registered User

Join Date: Aug 2007
Location: Montreal, Canada
Posts: 615

In your expression

(X^2*y^4 + x^3*y^2 + x^2*y^2 + x^3 – x^3*y^3) divided by (x^2*y^3 + x^3*y)

You can cancel out a factor of x^2 to obtain the equivalent expression

(y^4 + x*y^2 + y^2 + x – x*y^3) divided by (y^3 + x*y)

God bless you.

Blog this Post Reply Reply With Quote

10-19-2012, 04:25 AM #23

trurl_
Registered User

Join Date: Dec 2004
Posts: 133

CANCEL THE RSA CONFERENCE

The simplest formula I have derived to find a pattern in Prime numbers knowing the first and finding the second is:
Where x is the first Prime and y is the next Prime in the series.

[y = x^2*y^4+x^3*y^2+x^2*y^2+x^3] divided [x^2*y^3+x*y]

Example x =5, y=7
y = [25y^4 + 150y^2+125] / [25y^3+5y]
y = 7.83921 approximately 7

This is the easiest I can make the equation. Unfortunately I do not know any ways to deal with high exponents, but this is my concept simplified.

Stealth Coder know nearing 6 years what do think a pattern of Primes lies on a log spiral? If I have made you reconsider or second guess yourself, I have showed that impossible problems like Primes are impossible from looking for patterns in numbers. Instead look for a pattern in geometry. My methods are simple. But do you think they could be used for simplified attacks against RSA and the other one way functions that rely on Prime numbers.

I know it is a lot to theorize, but do you see any benefit to my work?

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

+ Reply to Thread

Page 3 of 3 | First | 1 | 2 | 3

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

Services
Live Classes
Workshops
Subscriptions
Support

News
Company Blog
Newsletter

Community
All Forums
General Discussion

Connect
Become a fan
Follow Us

Contact Us
About 3D Buzz

All times are in GMT 0