

Re: JSH: Contradictory behavior, issue of math fraud

Source: <http://sci.tech-archive.net/Archive/sci.math/2007-09/msg00477.html>

- *From:* rossum <rossum48@xxxxxxxxxxxxx>
 - *Date:* Mon, 03 Sep 2007 20:06:25 +0100
-

On Mon, 03 Sep 2007 15:25:47 -0000, JSH <jstevh@xxxxxxxxxx> wrote:

On Sep 3, 1:42 am, rossum <rossu...@xxxxxxxxxxxxx> wrote:

On Sun, 02 Sep 2007 10:19:32 -0700, JSH <jst...@xxxxxxxxxx> wrote:

But if the idea turns out to be a brilliant one which means factoring is not a hard problem after all, then how can mathematicians who not only couldn't figure it out, but who ignored it when presented with it be considered to be true experts in the field?

In its current version surrogate factoring is too slow to be considered "brilliant". Only when you have speeded it up sufficiently

I asked, what if?

Strictly, you said "But if ...". All I am pointing out that the "if" is still in the future, you are not there yet.

can it be considered brilliant. Slow factoring methods are a dime-a-dozen. The difficult part is finding a *fast* factoring method, that is a polynomial time rather than an exponential time method. So far your method seems to be exponential time, or do you have a proof that it is polynomial time?

If practicality is all that matters then acknowledge that "pure math"

Re: JSH: Contradictory behavior, issue of math fraud

is a bogus concept.

No, it is just that I am more focused on computing than on Pure Maths, so I tend towards the applied end of the spectrum. Hence my preference for actually coding something up and seeing what emerges. I leave the theory to other people.

In the real world, only math that is practical matters, which is a major point I'm making.

Both pure and applied have their places. I prefer applied, but today's pure is often tomorrow's applied.

Let's say that down the line someone proves that surrogate factoring not only is polynomial time, but that it blows away all other factoring approaches known, what does that say about the current math community's expertise in this area?

Surogate factoring is your baby, I suggest that *you* try proving that it is either exponential or polynomial time. If it turns out to be polynomial time then you are onto a winner. If it is exponential then that is an indication that this idea will probably not work out and you should look for a different approach.

If you want people to notice surrogate factoring then either factoring an RSA number or a proof that it works in polynomial time would be effective. As others have pointed out, all you have so far is "if". Anyone can have as many if's as they want. To be taken seriously you need to actually produce something from your surrogate factoring idea. If you don't want to factor an RSA number then a proof that surrogate factoring runs in polynomial time would do as well. A new polynomial time factoring method would be big news.

Note, I'm talking a hypothetical.

The question is, what if it turns out to be this incredibly powerful factoring technique that most of the math community ignored and people like you talked down?

How expert then could you really be?

I do not claim to be an expert. I merely crunch numbers for amusement in my spare time. I last did serious maths during my BSc degree back in the 1970s. My work since then has mostly been in computing, hence my interest in the computational utility of your idea.

Re: JSH: Contradictory behavior, issue of math fraud

Re: JSH: Contradictory behavior, issue of math fraud

rossum

[snip]

James Harris