

Re: Proof factoring solution is closed form

Source: <http://sci.tech-archive.net/Archive/sci.math/2005-02/3758.html>

From: Nora Baron (norabaron_at_hotmail.com)

Date: 02/11/05

Date: 10 Feb 2005 18:16:13 -0800

jstevh@msn.com wrote:

> *Tim Peters wrote:*

> > [JSH]

> > > ...

> > > *I say, quit hiding things, put up your example where I can see it,*

> *like*

> > > *in a thread where I'm paying attention, as if you're right I'd like*

> *to*

> > > *know.*

> >

> > *Rick replied in one of the threads you started. How is he supposed*

> *to guess*

> > *which of those you pay attention to? If you're so bored by your*

> > *proliferation of redundant threads that you don't pay attention to them*

> > *anymore, and are too lazy to do a simple search, tough luck.*

> >

>

> *I don't need luck. Remember I'm the inventor of surrogate factoring.*

>

> *And I mentioned in an earlier post that I'd tested out this latest*

> *twist on my own idea and found it didn't work, over the weekend.*

>

> *So, deep down some part of me knew it didn't work anyway, so it wasn't*

> *worth the effort to try and find some post out in the haystack.*

>

Ridiculous. The post was a very recent one in one of a few threads you started in the last day or two. Given that Rick Decker was the author, finding it would be no trouble at all.

> *Nonetheless talking it out paid dividends as the full solution was just*

> *an inversion away.*

>

sci.math: Re: Proof factoring solution is closed form

- > *I find it interesting that no one else thought to just invert x , and*
- > *pull out the complete solution, but I seem to have a gift for this*
- sort
- > *of thing.*
- >
- > *And yes, in case you're wondering, I did find a short proof of*
- Fermat's
- > *Last Theorem,*

No, you absolutely did not.

- > *and I did find THE prime counting function,*

No again. What you found was an *algorithm* which computes values of the prime counting function.

- > *though people*
- > *don't seem to realize its importance for some reason, though it has*
- > *application in number theory and physics,*

The prime counting function itself may be "useful" or at least interesting. Your algorithm for computing it is essentially, as YOUR OWN Wikipedia article said, an inclusion–exclusion algorithm and closely related to Legendre's algorithm. As such, it is asymptotically slower than other more recent methods. It was obsolete before you even wrote it. Plus you have not shown that it has any theoretical implications.

- > *and I did find a problem in*
- > *algebraic number theory with erroneous thinking by mathematicians*
- over
- > *a hundred years ago that lasted to this day.*
- >

No, this too is absolutely wrong, and you have seen proofs of it.

- > *That's not even all, as I have work in logic that I just don't bother*
- > *discussing.*
- >
- > *I have more discoveries that I simply don't see the point in talking*
- > *about, as people find it hard to comprehend the simple ones.*
- >
- > *There is no reason that a sane world should have left me to fiddle*
- with
- > *the factoring problem as there was every reason to believe that I*
- would
- > *succeed, and with a very basic solution, which I did.*
- >

Whether your approach to factoring leads to anything remains to be seen. You replace factoring a large number M with factoring of

a number $T = M^2 - j^2$, where in general you might choose j to be relatively small. There are two possibilities regarding T which need to be considered. One is that it has two or more extremely large prime factors, very possibly with almost twice the digit-length of the factors of M itself. If this happens, it will likely be harder to find them than it would be to find the prime factors of the original M . Two is the possibility that T has a great many small prime factors. In that case, the number of possible integer divisors of T could be very large, and searching through all of them might take as much time as factoring M in the first place, and may not work anyway. You do not have a proof that it has to work. You do not have a proof that it has to work in polynomial time. The real test for you is, can you factor a sizeable RSA number? If you cannot, no amount of bragging and counting-chickens-prematurely is going to do you any good or impress anybody. If you can, you will be in fat city. How should you be spending your time? Calumny, or calculating?

> *You people had no good reasons to let this happen this way.*
>

??? You mean, someone should have stopped you ???

> *But you did--seeming to enjoy insulting me more than anything else,*
> *which I find frustrating as you seem to be weird little children with*
> *barely even a basic comprehension of mathematics--and now the full*
> *solution to the factoring problem is not only known, but easily*
> *implemented, as the math is childishly simple.*
>

You made a barbarically rude comment to Rick Decker. He has been unfailingly polite and reasonable and has done a far better job than you have yourself of explaining what you are trying to do. You pay him back with sheer meanness. You should be ashamed, and you owe him an apology.

Nora B.

>
> *James Harris*