

Re: Easy test of surrogate factoring

Source: <http://sci.tech-archive.net/Archive/sci.math/2005-02/6939.html>

From: David C. Ullrich (ullrich_at_math.okstate.edu)

Date: 02/18/05

Date: Fri, 18 Feb 2005 08:25:07 -0600

On 18 Feb 2005 04:25:13 -0800, jstevh@msn.com wrote:

>Paul Rubin wrote:

>> Here's an even easier test of surrogate factoring: I gave you a list
>> of fifty 20-digit composite numbers a couple weeks ago and you
>haven't
>> factored a single one. I think I know what test score to assign,
>> based on that result.

>

>No, it's not a fair test.

Wondering whether a new and earthshattering factoring method
can be used to factor numbers is not a fair test? Huh.

>I'll explain why,

Ok...

>again, and I'll also

>explain again, what the test is, and why my test is an easy one.

>

> $Ax = Az(-Az \pm \sqrt{(Az - 2M^2)^2 - 4TM^2}) / (2j^2 - 2Az)$

>

> $Az = Ax(-Ax \pm \sqrt{(Ax - 2j^2)^2 + 4Tj^2}) / (2M^2 - 2Ax)$

>

>shows that you have a set of rational Ax mapped to rational Az

>solutions, where you have dependencies on the factorizations of TM^2

>and Tj^2 to make the square roots rational.

>

>Notice, you are guaranteed to have an integer Az that factors M , from

>the first equation, which gives a rational Ax , and searches for

>algorithms are basically about figuring out how to get all the possible

>integer Az 's.

>

>However, you can do the time honored technique of working backwards to

>see actual solutions, as is easily calculated if you *do* know the

>prime factors of M , as then you can just pull out all the integer Az 's

>from the first equation.

sci.math: Re: Easy test of surrogate factoring

>

>*It's a well-known technique to work backwards to figure out what's*
>*going on.*

>

>*My test is to work backwards.*

>