

Re: which schools research factoring?

Re: which schools research factoring?

Source: <http://sci.tech-archive.net/Archive/sci.math/2007-08/msg05487.html>

- *From:* Pubkeybreaker <pubkeybreaker@xxxxxxx>
 - *Date:* Fri, 31 Aug 2007 05:32:35 -0700
-

galathaea wrote:

On Aug 30, 6:03 pm, ToddSmith <ellipt...@xxxxxxxxxx> wrote:

Hi,

I just got my Master's degree at an applied-leaning school and I want to research the problem of factoring large integers somewhere else for a PhD. Which school are doing the most research in factoring these days?

while hendrik is over at berkeley

Nope. He left. He is back in the Netherlands full time.

The difficulty with "researching factoring" is that it is not really a problem in which a dedicated effort will lead to results. A new factoring algorithm seemingly requires a new piece of inspiration. It is impossible to predict when such a thing will occur.

Of course one can find incremental improvements to existing algorithms (I just published one such paper and am working on extending it; I gave a rump talk at Crypto), but it seems unlikely that this type of thing would be accepted as a PhD thesis. OTOH, Peter's thesis was on applying FFT techniques to ECM, so it can be done.

If you really want to do this sort of thing, you should look at CWI and Lausanne. You should also seek out Franke and Kleinjung. While the TOC group at MIT is quite good, this is not really their domain. And (AFAIK) people at Waterloo are not really pursuing it either.

If you want to do this sort of thing, you really need a general PhD in

Re: which schools research factoring?

Re: which schools research factoring?

number theory to go along with it.