

Re: Factorisation algorithms

Source: <http://sci.tech-archive.net/Archive/sci.math/2007-10/msg02457.html>

- *From:* Chip Eastham <hardmath@xxxxxxxx>
 - *Date:* Tue, 16 Oct 2007 21:16:24 -0000
-

On Oct 16, 3:56 pm, matt271829-n...@xxxxxxxxxxxx wrote:

Has anyone ever proved any theoretical bounds on the efficiency of a general integer factorisation algorithm? Is it still, as far as anyone knows, possible that a really spectacular advance might be made in this field?

Yes, as far as I know, it seems entirely possible that deterministic algorithms may be found with complexity comparable to the heuristic/probabilistic behavior of the current best algorithm, the general number field sieve.

A survey of results through the 20th century is here:

<http://algo.inria.fr/seminars/sem00-01/morain.html>

regards, chip

.