

# Re: Factorisation algorithms

---

*Source:* <http://sci.tech-archive.net/Archive/sci.math/2007-10/msg03021.html>

---

- *From:* [ime@xxxxxxxxxx](mailto:ime@xxxxxxxxxx) (Randy Hudson)
  - *Date:* Wed, 17 Oct 2007 04:23:53 +0000 (UTC)
- 

In article <1192584825.140877.253980@xxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxx>, <matt271829-news@xxxxxxxxxxx> wrote:

He also cites Shamir, *Inf. Proc. Letters* 8 (1979), pp 28–31, for a demonstration that, if the processing time for an arithmetic operation is independent of the size of the numbers involved, then  $N$  can be factored in at most  $O(\ln(N)^2)$  times that processing time.

I have a feeling that this might be a very stupid question, but, even allowing for the fact that in reality arithmetic takes longer for larger numbers, isn't  $O(\ln(N)^2)$  still very much better than any known algorithm? I'm assuming that the numbers involved are at worst  $O(N)$ .

The numbers involved are  $O(N!)$ ; that's  $O((N/e)^N)$ .

—  
Randy Hudson