

## Re: factorization an NP problem (don't see it)

---

*Source:* <http://sci.tech-archive.net/Archive/sci.math/2006-07/msg00886.html>

---

- *From:* [stephen@xxxxxxxxxxx](mailto:stephen@xxxxxxxxxxx)
  - *Date:* Thu, 6 Jul 2006 05:23:43 +0000 (UTC)
- 

oferlock@xxxxxxxxxxx wrote:

factorization as a decision problem : given a composite integer  $m$  and  $k < m$ , does  $m$  have a non-trivial factor less than  $k$ ?  
this is an NP problem, since given an integer (witness),  $w$ , such that  $w \leq k$ , we can check by long-division if  $w$  is a factor of  $m$ . My dilemma :  
if this can be done for all integers upto  $k$  in polynomial time  $O(n^t)$ , then we can check each of the integers upto  $k$  and that's only a factor of  $n$  (at most) slowdown. i.e, still  $O(n^{t+1})$ . Where is the catch?

What are  $n$  and  $t$ ? You describe a problem where you are given  $m$  and  $k$ , but then describe the running time as  $O(n^t)$ .

Anyway, the short answer is that the running time needs to be expressed in terms of the size of the problem. The size of an instance of factorization is the number of bits needed to represent  $m$  and  $k$ . So the size of the problem is  $O(\log m)$ . A running time of  $O(m)$  is exponential with respect to the size of the problem.

Stephen

.