

factorization an NP problem (don't see it)

Source: <http://sci.tech-archive.net/Archive/sci.math/2006-07/msg00872.html>

- *From:* oferlock@xxxxxxxxxx
 - *Date:* 5 Jul 2006 21:16:28 -0700
-

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?

.