

Silly Factoring Theorems

Source: <http://sci.tech-archive.net/Archive/sci.math/2005-05/msg00000.html>

- *From:* "rich burge" <r3769@xxxxxxx>
 - *Date:* 30 Apr 2005 14:24:51 -0700
-

jst...@xxxxxxx wrote:

- >
- > So your position is that only practicality matters.
- >
- > In this case that position is that only if there is a real world use
- > for the SFT is it valuable.
- >

Silly factoring theorems (sft's) are a dime a dozen. For example, suppose $n=p*q$ is given where p and q are unknown primes. Further, suppose p is k digits long. Then one example of a sft is the following:

Thm: There exists a natural number e such that the leading k digits of n^e are equal to (the k digits of) p .

Sft's are many, but this one is somewhat curious, simple to prove(?), and decidedly silly. Thus it meets and exceeds all the requirements of a good sft. However, if one was able to prove, say, that $e < P(k)$, for some polynomial P , then this particular sft would be a *lot* more interesting, perhaps even useful. Utility is decidedly NOT a requirement to be a sft, but it is, I suppose, possible some sft is useful.

So how could one go about proving $e < P(k)$? One approach is to first find some evidence that it is true: i.e. perform some experiments! This is where "practicality matters". Is it wise to start experimenting with one of the RSA challenge numbers? No, that's dumb, and those who would offer such advise for this or any other sft are themselves being silly (or cruel).

The professional mathematician would probably quickly recognize that no such P could exist and thus avoid the need for such amateurish experimentation, but that is another matter.

Rich

.

- *Follow-Ups:*
 - ◆ *Re: Silly Factoring Theorems*
 - ◇ *From:* Mark Atherton
- Next by Date: *Re: Question about sets of functions*
- Next by thread: *Re: Silly Factoring Theorems*
- Index(es):
 - ◆ *Date*
 - ◆ *Thread*