

# Re: factorization

---

*Source:* <http://www.derkeiler.com/Newsgroups/sci.crypt/2007-05/msg13355.html>

---

- *From:* Pubkeybreaker <[pubkeybreaker@xxxxxxx](mailto:pubkeybreaker@xxxxxxx)>
  - *Date:* 17 May 2007 11:09:40 -0700
- 

Douglas A. Gwyn wrote:

Mirror wrote:

All prime numbers – except 2 and 5 – have as their last digit, either 1 or 3 or 7 or 9.

Duh.

We notice that the last digit of the multiplication of two prime numbers is also 1,3,7 or 9. How is that ?

False:  $5 * 7 = 35$ , last digit is 5  
 $2 * 3 = 6$ , last digit is 6

...  
this fact can possibly lead to a factorization in polynomial time or even faster.

Many people have tried a more sophisticated analysis of the low- and high-order digits (usually bits, rather than decimal digits) but haven't yet been able to turn the idea into a practical factoring algorithm.

In fact, it can NOT lead to a P-time method. (unless  $P = NP$ )

Attempts to "reverse" the multiplication process by looking at the digits leads to a system of diophantine equations whose solution is known to be NPC. The basic problem is that one gets an "exponential explosion" of possible answers when analyzing the carries.

Re: factorization