

## Re: A very fast Fermat factoring algorithm

**Source:** <http://www.derkeiler.com/Newsgroups/sci.crypt/2005-03/2374.html>

---

**From:** quantumgecko (*pete2498\_at\_umn.edu*)

**Date:** 03/30/05

Date: 30 Mar 2005 08:44:06 -0800

Pubkeybreaker wrote:

> *In fact, there are a several known techniques to speed Fermat  
> factoring.*  
>  
> *Another is a very old technique that uses exclusion moduli to  
restrict  
> the  
> search space. If we have  $x^2 - y^2 = N$ , then  $x$  is a quad. res. One  
> can look at  
>  $N \bmod$  various primes. Then  $x$  modulo those primes must be a quad.  
res.*

I'd rather not share the technique just yet. I don't know for sure if it has any value. I will say though that about  $\sim 10^6$  of my speed up is a space/time trade-off and about  $\sim 10^3$  of it is an "exclusion moduli" thing, although mine doesn't use quadratic residues. I'll have to check, it's possible it's the same technique in disguise.

I have heard of several Fermat speedups, but none that are nearly this fast. I also know of no method of space/time trade-off for Fermat's algorithm besides this.

What I mean by "equivalent to Fermat's" is that it looks absolutely nothing like Fermat's algorithm, but it has the same runtime expression: # iterations =  $c(\sqrt{p} - \sqrt{q})^2$  except that  $c=0.5$  for Fermat and  $c=10^{-9}$  for me. I think the iterations are faster too.

I compared my algorithm to Pollard rho for my paper. Pollard rho searches small factors fast, my algorithm searches big factors fast, so this was an interesting test of usefulness. My algorithm beats Pollard Rho on numbers from 15 to 40 decimal digits when  $0.1 < p/q < 10$ , that is, when the two primes have about the same number of decimal digits. Other Fermat-like algorithms are much more strict about the closeness of  $p$  and  $q$ .

Thank you for your comments.