

## Re: Factoring problem solution

**Source:** <http://sci.tech-archive.net/Archive/sci.math/2005-02/6930.html>

---

**From:** Dik T. Winter (*Dik.Winter\_at\_cwi.nl*)

**Date:** 02/18/05

Date: Fri, 18 Feb 2005 13:39:41 GMT

In article <1108112043.489072.164510@c13g2000cwb.googlegroups.com> "tomstdenis@gmail.com" <tomstdenis@gmail.com> writes:

...

>  $x^2 - y^2 == 0 \pmod{N}$  and  $x \neq y$  then you have a good chance of  
> factoring  $N$ .

In practise, when  $x \neq y$ , and when  $N$  has only two factors, the probability to obtain non-trivial factors is about 1 in 2. (It gets better when  $N$  has more factors.) That is the reason that MPQS algorithms in general generate quite a few more basic relations than actually needed. If you have  $N$  basic relations with a factor base of  $M$  primes, when  $N > M$  you will find  $(N-M)$  (different) relations of the form  $x^2 - y^2 == 0 \pmod{N}$ . So getting to  $N = M + 100$  will almost surely factor the number.

--

dik t. winter, cwi, kruislaan 413, 1098 sj amsterdam, nederland, +31205924131  
home: bovenover 215, 1025 jn amsterdam, nederland; <http://www.cwi.nl/~dik/>