

## Re: JSH: Difference of squares

**Source:** <http://sci.tech-archive.net/Archive/sci.math/2005-03/7569.html>

---

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

**Date:** 03/22/05

Date: Tue, 22 Mar 2005 02:34:43 GMT

In article <1111455854.608236.182810@f14g2000cwb.googlegroups.com> jstevh@msn.com writes:

> *Consider*

>

>  $x(x+a) = M$

>

> *where M is your target, as then you can use the quadratic formula to*

> *solve for x, and get*

>

>  $x = (-a \pm \sqrt{a^2 - 4M})/2$

>

> *and most of the work in factoring has to do with figuring out some a,*

> *such that the square root is an integer, and you factor M.*

This is wrong. You start with  $(y-b)(y+b) = M$ , and do not need the quadratic formula, Fermat did that already. Note that in your formula, 'a' is always even (because 'M' is odd), so can be replaced by '2b' for some integer 'b'. And now  $y = x + b$ .

And in current work 'b' is not necessarily an integer, but can be an algebraic integer (as can be 'y'). (Look for the Number Field Sieve.) Strange enough, although there is apparently a flaw in the algebraic integers, using them made it possible to factor quite large numbers. RSA-130 was the first major one, I think.

--

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